

SkyMesh HYC-OLTRG-100gn-27

Outdoor 4G/LTE Router with 2.4GHz Wi-Fi



User Manual

Includes install, configuration and trouble shooting information for the broadband wireless access outdoor radio.

Table of Contents

1	Introduction.....	5
1.1	Features	5
1.2	Hardware Interface.....	6
1.3	Hardware Interface Introduction	7
2	Hardware Installation.....	8
2.1	LED Indicators	8
2.2	Reset Button (RST).....	8
2.3	Ethernet Port	9
2.4	Install the SIM Card (Micro-Sim).....	9
2.5	External Antenna.....	10
2.6	Connecting the Power Supply	10
3	Configuration via Web Browser.....	11
4	Status	12
4.1	Status > GPS.....	13
5	Configuration > System	15
5.1	System > Time and Date	15
5.2	System > Logging.....	19
5.2.1	Logging > Logging	19
5.2.2	Logging > Log.....	20
5.3	System > Alarm	21
5.3.1	Alarm > Name Group	22
5.3.2	Alarm > Edit User.....	22
5.4	System > Ethernet Ports	24
5.5	System > Client List	24
6	Configuration > WAN.....	26
6.1	WAN > Priority	26
6.2	WAN > Ethernet	26
6.2.1	WAN Ethernet Configuration.....	26
6.2.2	Ethernet Ping Health.....	29
6.3	WAN > IPv6 DNS.....	30
7	Configuration > LTE.....	32
7.1	LTE > LTE Config.....	32
7.1.1	LTE Configuration	32
7.1.2	LTE Ping Health.....	33
7.2	LTE > Dual SIM.....	34
7.3	LTE > Usage Display.....	38
7.4	LTE > SMS	41

8	Configuration > LAN	43
8.1	LAN > IPv4	43
8.2	LAN > IPv6	44
8.3	LAN > VLAN	44
8.4	LAN > Subnet	46
9	IP Routing	48
9.1	IP Routing > Static Route	48
9.2	IP Routing > RIP	50
9.3	IP Routing > OSPF	52
9.4	IP Routing > BGP	56
10	Configuration > Service	59
10.1	Service > Configuration OpenVPN	59
10.1.1	Edit OpenVPN Connection	59
10.1.2	Set up OpenVPN Client	62
10.1.3	Set up OpenVPN Server	63
10.1.4	Set up OpenVPN Custom	64
10.2	Service > Configuration IPsec	66
10.2.1	IPsec > General setting	66
10.2.2	IPsec > Connections	68
10.2.3	IPsec > The setting of X.509 Certificates	69
10.2.4	IPsec > Net-to-Net Configuration	70
10.3	Service > Configuration Port Forwarding	75
10.4	Service > Dynamic DNS	76
10.5	Service > DMZ	78
10.6	Service > SNMP	78
10.6.1	SNMP configuration	78
10.6.2	SNMP v3 User configuration	79
10.6.3	SNMP trap configuration	80
10.7	Service > TR069	81
10.8	Service > IP Filter	82
10.9	Service > MAC Filter	84
10.10	Service > URL Filter	85
10.11	Service > VRRP	86
10.12	Service > MQTT	87
10.13	Service > UPnP	89
10.14	Service > SMTP	89
10.15	Service > NAT	90
10.16	Service > IP Alias	90
10.17	Service > GRE	91
11	Management	92
11.1	Identification	92

11.2	Administration	93
11.3	Firmware.....	93
11.4	Configuration	93
11.5	Load Factory	94
11.6	Restart	94
12	Configuration Applications	95
12.1	WAN Priority	95
12.2	LAN > IPv4/IPv6 Dual Stack	97
12.3	MQTT Broker	98
12.4	OpenVPN Configuration	99
12.4.1	OpenVPN Server Mode	99
12.4.2	OpenVPN Client Mode.....	100
12.4.3	OpenVPN Net-to-Net	101
12.4.4	OpenVPN 1:1 NAT	104
12.4.5	OpenVPN with third-party server.....	105
12.5	VRRP Topology	106
12.6	TR069 Server (GenieACS Installation).....	107

1 Introduction

Hypercable HYC-OLTRG-100 series 4G/LTE 4G/LTE Router are highly reliable and secure wireless communications gateway designed for industrial networking. It supports multi-band connectivity including FDD/TDD LTE, WCDMA and GSM for a wide range of applications and vertical machine-to-machine (M2M) markets. To enhance reliability, **HYC-OLTRG-100** series are equipped with dual SIM that support failover and roaming over to ensure uninterrupted connectivity for mission-critical cellular communications.

With flexible LAN/WAN Ethernet options, **HYC-OLTRG-100** series allow you to customize your professional applications in diverse environments. Integrated with WAN, LAN, the **HYC-OLTRG-100** series also provide various network protocols, such as IPv6, MQTT and VPN for enriching connectivity and security. For VPN tunnel, OpenVPN and IPSec are for reliable authentication of the network stations, data encryption and verification of data integrity. The device is administrated via web GUI, Telnet, SSH v2 and HTTP/HTTPS.

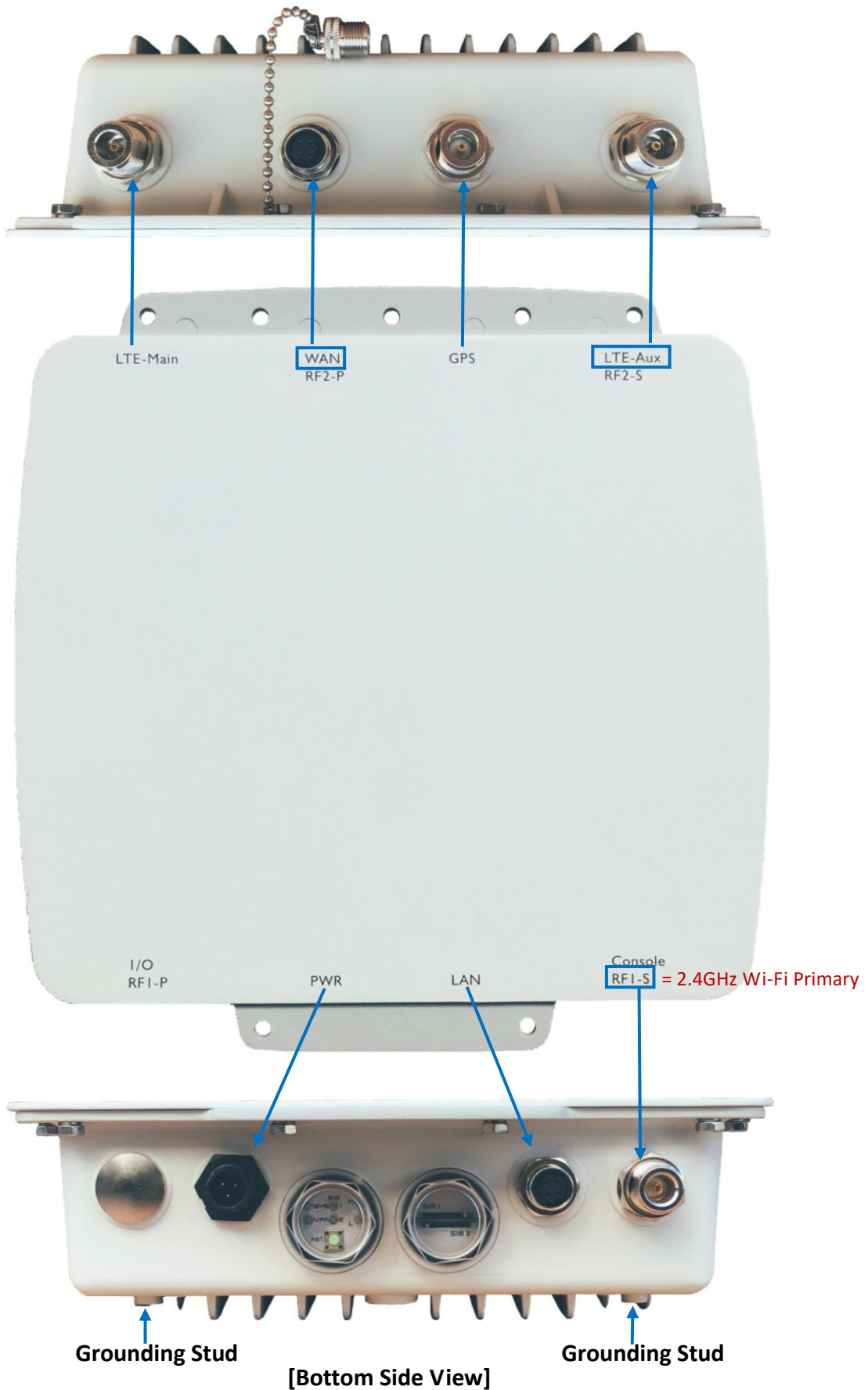
Built for secure and uninterrupted operation in harsh environments, **HYC-OLTRG-100** series support extended operating temperature from -20 to +70°C and IP-68 grade water and dust proof outdoor enclosure.

1.1 Features

- Highly reliable and secure for mission-critical cellular communications
- Provide flexible options to configure LAN/ WAN ports
- Support multi-band connectivity with FDD LTE/ TDD LTE/ WCDMA/ GSM/ LTE Cat4
- Built-in dual SIM for network redundancy
- Integrated dual detachable antenna against radio interference
- LED indicators for connection and data transmission status
- Industrial rated from -20°C to +70°C for use in harsh environments
- Aluminum diecasting outdoor enclosure with IP68 industrial grade protection
- IPv6/IPv4 dual stack and all applications are IPv6 ready
- Support various serial communication protocols for connectivity
- Enhance security and encryption for authentication and transmission

1.2 Hardware Interface

[Top Side View]



1.3 Hardware Interface Introduction

[Top Side View]

Interface	Description
LTE-Main	Connect to LTE antenna with N-type connector
WAN	Connect to Ethernet Cable with M12 connector
GPS	Connect to GPS antenna with N-type connector
LTE-Aux	Connect to LTE antenna with N-type connector

[Bottom Side View]

Interface	Description
PWR	Connect to Power cable with Circle-B type connector
LAN	Connect to Ethernet Cable with M12 connector
LED Indicators	SYS / VPN / SIM1 / SIM2 / H (RSSI) / L (RSSI)
RST	Allows you to reboot the unit or restore to factory default setting. Reboot - Press the button for 1 second Restore to factory default setting - Press the button for 5 seconds
SIM1 & SIM2	Insert the Micro Sim Card (Push – Push Sim Card holder)
RF1-S	2.4GHz Wi-Fi Primary port – Connect to 2.4GHz antenna with N-type connector
Grounding stud	Connect to the ground wire with stainless screws.



Ethernet Cable with **M12** connector connector



Power Cable with **Circular Standard (CCB)**

2 Hardware Installation

This chapter introduces how to install and connect the hardware.

2.1 LED Indicators



LED	SYS	H (RSSI)	L (RSSI)	VPN	SIM1	SIM2
ON	System UP	Normal Signal	Low Signal	VPN Connected	Connected	Connected
Slow Blinking	Booting	N/A	N/A	WAN Connected	Connecting	Connecting
Fast Blinking	N/A	N/A	N/A	N/A	Error	Error
OFF	Power Down	N/A	N/A	NO WAN Connection	Not Working	Not Working
Heart Beat	N/A	N/A	N/A	N/A	Reading	Reading

2.2 Reset Button (RST)

Reset button allows you to reboot the unit or restore to factory default setting.

Function	Operation
Reboot	Press the button for 1 second
Restore to factory default setting	Press the button for 5 seconds

Note:

Press the Reset button and count the time around 5 seconds. The LED Indicators will be blinking to show you have activated the setting successfully.

2.3 Ethernet Port

(1) 10/100 Mbps Ethernet WAN

Pin	Description	Function
1	WAN TX+	10/100 Mbps WAN, TX+ Pin
2	WAN TX-	10/100 Mbps WAN, TX- Pin
3	WAN RX+	10/100 Mbps WAN, RX+ Pin
4	N/A	N/A
5	N/A	N/A
6	WAN RX-	10/100 Mbps WAN, RX- Pin
7	N/A	N/A
8	N/A	N/A

(2) 10/100 Mbps Ethernet LAN

Pin	Description	Function
1	LAN TX+	10/100 Mbps LAN, TX+ Pin
2	LAN TX-	10/100 Mbps LAN, TX- Pin
3	LAN RX+	10/100 Mbps LAN, RX+ Pin
4	N/A	N/A
5	N/A	N/A
6	LAN RX-	10/100 Mbps LAN, RX- Pin
7	N/A	N/A
8	N/A	N/A

2.4 Install the SIM Card (Micro-Sim)



1. Push-Push Sim Card holder for Micro-Sim Card

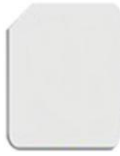


Note:

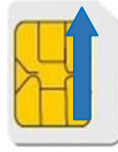
- If you are using Nano – Micro adaptor as Micro-Sim, please use the sticker to stick the Nano Sim card and adaptor together.

2. Insert and Remove SIM1/SIM2 Card

- (1) Before inserting or removing the SIM card, ensure that the power has been turned off and the power connector has been removed from 4G/LTE Router.
- (2) Insert the Micro - SIM card into the push-push Sim card holder by following instruction.



SIM1 (chip side down)



SIM2 (chip side up)

- (3) Insert the SIM card with the contacts facing up and align it properly into the drawer. Make sure your direction of SIM Card and put it into the tray.
- (4) Slide the drawer back and locks it in place.

Note:

- Please make sure the insert direction is correct first. When pulling the Micro-SIM card from the tray by incorrect direction, the chip card or the tray might be damaged.
- Please turn off your router before insert or remove the SIM card.

2.5 External Antenna

Each unit has two antenna connectors (SMA), MAIN and AUX. Connect the antenna to MAIN when you have only one antenna. Please tighten the connecting nut properly to ensure good connection.

2.6 Connecting the Power Supply

The router requires a DC power supply in the range of 24V DC. Please ensure all components are earthed to a common ground before connecting any wiring.



Wire color	DC Power (24V)
Yellow	Chassis Ground
White	V -
Black	V+

Note:

- Please make sure the power voltage and polarization are correct and match with the wire color.

3 Configuration via Web Browser

Access the Web Interface

4G/LTE Router:

The web configuration is an HTML-based management interface for quick and easy set up of the 4G/LTE Router. Monitoring of the status, configuration and administration of the router can be done via the Web interface.

After properly connecting the hardware of 4G/LTE Router as previously explained. Launch your web browser and enter <http://192.168.1.1> as URL.

The default IP address and sub net-mask of the 4G/LTE Router are 192.168.1.1 and 255.255.255.0. Because the 4G/LTE Router acts as DHCP server in your network, the 4G/LTE Router will automatically assign IP address for PC or NB in the network.

Control Panel > Selecting Language

You can choose the languages, including English and Taiwan.



A screenshot of a language selection dropdown menu. The word "Language" is on the left, and "English" is selected in the dropdown, with a small downward arrow to its right.

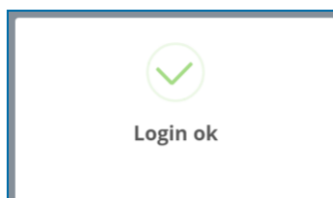
Logging in the Router

In this section, please fill in the default User Name **root** and the default Password **2wsx#EDC** and then click **Login**. For the system security, suggest changing them after configuration.

After clicking, the interface shows **Login ok**.



A screenshot of the router's login page. The page has a blue header with the word "Login". Below the header, there are two input fields: "User Name" with the text "root" and "Password" with asterisks. A blue "Login" button is located at the bottom right of the form area.



2.4GHz Wi-Fi AP:

IP address: **192.168.1.2**

User Name: **root**

Password: **2wsx#EDC**

4 Status

When you enter the web browser in the beginning, the interface displays the status of router to make you know about Cellular Attribute, Dual SIM information, the current connectivity of WAN Ethernet and LAN Ethernet. If you router with GPS function, the GPS interface is shown.

The screenshot shows the 'Mobile Router' web interface. The top navigation bar includes the router name, signal strength, carrier (Far EasTone), system uptime (07:50), WAN priority (LTE Only), location (24.77, 121.01), Google Maps, language (English), and a logout button. The main content area is divided into several sections:

- Status** (highlighted in red): A sidebar menu with options for System, WAN, LAN, Service, and Management.
- WAN LTE**: A table showing SIM card information (SIM2), modem status (Ready), operator (Far EasTone), access type (FDD LTE), IMSI (466011100041467), phone number, band (LTE BAND 3), channel ID (1550), and IPv4 address/mask (10.26.211.187 / 255.255.255.255).
- GPS**: A table showing location data: Latitude (24.774059295654297), Longitude (121.00943756103516), Horizontal (1.2000000476837158), Altitude (145), Date(UTC) (17/07/20), and Satellite (9).
- WAN Ethernet**: A table showing WAN IPv4 address (36.229.58.231) and mask (255.255.255.255).
- WAN DNS**: A table showing IPv4 and IPv6 DNS server addresses.
- LAN Ethernet**: A table showing LAN IPv4 address (192.168.1.1), mask (255.255.255.0), and IPv6 address (2001:b011:7000:f3c::100).

Status > WAN LTE	
Item	Description
Attribute	
SIM Card	Show the SIM card which the router work with currently: Current SIM or Backup SIM.
Modem Status	Show the status of modem.
Operator	Display the name of operator.
Modem Access	Show the router to access protocol type
IMSI	Show the IMSI number of the current SIM cards.
Phone Number	Show the phone number of the current SIM or Backup SIM.
Band	Show current connected Band.
Channel ID	Show current connected channel ID.
IPv4 Address	LTE obtain IPv4 address.
IPv4 Mask	LTE IPv4 mask.

Status > WAN Ethernet	
Item	Description
Attribute	
IPv4 Address	Ethernet WAN obtain IPv4 Address.
IPv4 Mask	Ethernet WAN obtain IPv4 Mask.

Status > LAN Ethernet	
Item	Description
Attribute	
IPv4 Address	Ethernet LAN is assigned IPv4 Address.
IPv4 Mask	Ethernet LAN is assigned IPv4 Mask.
IPv6 Address	Ethernet LAN is assigned IPv6 Address.

Status > WAN DNS	
Item	Description
Attribute	
IPv4 DNS Server #1	Show the address of IPv4 DNS Server #1.
IPv4 DNS Server #2	Show the address of IPv4 DNS Server #2.
IPv4 DNS Server #3	Show the address of IPv4 DNS Server #3.
IPv6 DNS Server #1	Show the address of IPv6 DNS Server #1.
IPv6 DNS Server #2	Show the address of IPv6 DNS Server #2.
IPv6 DNS Server #3	Show the address of IPv6 DNS Server #3.

Status > GPS	
Item	Description
Attribute	
Latitude	Show the latitude information of location.
Longitude	Show the longitude information of location.
Horizontal	Show the horizontal information of location.
Altitude	Show the altitude information of location.
Date(UTC)	Show the date information of location.
Satellite	Show the satellite information of location.

4.1 Status > GPS

For those GPS enabled router, you can see [Location](#) on the right-top banner of web interface when connecting your GPS function. After clicking this banner, a map will automatically display the current information of map according to location of router.

Status
System

Status



Attr.	Current SIM	Backup SIM
	SIM1	SIM2
	Ready	Not Inserted
	Chunghwa Telecom	
	FDD LTE	
	466924290355496	
	LTE BAND 7	
	3050	0
	10.162.241.68	
	255.255.255.255	

Value

Ethernet LAN

Attr.	Value
IPv4 Address	192.168.1.1

5 Configuration > System

This system section provides you to configure the following items, including Time and Date, Logging, Alarm, Ethernet Ports, RIP.



5.1 System > Time and Date

This section allows you to set up the time and date of router and NTP server. There are two modes at Time and Date Setup, including **Get from Time Server** and **Manual**. The default mode is **Get from Time Server**.

If the router has GPS function, you can turn on "**GPS Time**" for sync time from GPS server.

For **Time Zone Setup**, the **Daylight Savings Time** allows the device to forward/backward the amount of time from **Ahead of standard time** setting automatically when the time is at the **Daylight Savings** duration that you have set up before.

I. Get from Time Server

- Set up the time servers of IPv4 and IPv6.
- Select your local time zone.
- Click to keep your configuration settings.

Time And Date

Current Time Dec 4, 2017 10:15:29 AM

Time and Date Setup

Mode Manual Get from Time Server

GPS Time Off On

IPv4 Server #1

IPv4 Server #2

IPv4 Server #3

IPv6 Server #1

IPv6 Server #2

IPv6 Server #3

Time Zone Setup

Time Zone

Daylight Savings Off On

Ahead of standard time mins

Start Date / / (Month / Week / Day)

Start Time : (Hour : Minute)

End Date / / (Month / Week / Day)

End Time : (Hour : Minute)

Apply

II. Manual

- Set up the information of time and date, including year, month, date, and hour, minute, and second.
- Set up your local time zone.
- Click **Apply** to submit your configuration changes.

🏠 Time And Date

Current Time Dec 4, 2017 10:20:54 AM

Time and Date Setup

Mode Manual Get from Time Server

GPS Time Off On

YYYY-MM-DD - - HH:MM:SS : :

Time Zone Setup

Time Zone

Daylight Savings Off On

Ahead of standard time mins

Start Date / / (Month / Week / Day)

Start Time : (Hour : Minute)

End Date / / (Month / Week / Day)

End Time : (Hour : Minute)

Apply

III. Time Zone Setup

- Set up **Daylight Savings** as On.
- Set up **Ahead of standard time**.
- Set up the information of Start Date/Time, including Month, Week, Day, Hour and Minute.
- Set up the information of End Date/Time, including Month, Week, Day, Hour and Minute.
- Click Apply to submit your configuration changes.

Time Zone Setup

Time Zone

Daylight Savings Off On

Ahead of standard time mins

Start Date / / (Month / Week / Day)

Start Time : (Hour : Minute)

End Date / / (Month / Week / Day)

End Time : (Hour : Minute)

Apply

System > Time and Date->Daylight Savings	
Item	Description
Daylight Saving	Turn on/off the Daylight Savings feature. Select from Off or On. The default is Off.
Ahead of standard time	The forward/backward minutes when enter/leave Daylight Savings duration.Default is 60 mins.
Start Date/Start Time	<p>Time to enter Daylight Savings duration. The Month range is 1~12;</p> <ul style="list-style-type: none"> 1 - Jan. 2 - Feb. 3 - Mar. 4 - Apr. 5 - May 6 - Jun. 7 - Jul. 8 - Aug. 9 - Sep. 10 - Oct. 11 - Nov. 12 - Dec. <p>The Week range is 1~5;</p> <ul style="list-style-type: none"> 1 - first week in month. 2 - second week in month 3 - third week in month 4 - fourth week in month 5 - fifth week in month <p>The Day range is 0~6;</p> <ul style="list-style-type: none"> 0 - Sunday(The start day of a week) 1- Monday 2 - Tuesday 3 - Wednesday 4 - Thursday 5 - Friday 6 - Saturday <p>The Hour range is 0~23; The Min range is 0~59;</p>
End Date/End Time	Time to leave Daylight Savings duration. Same with Start Date/Start Time.

5.2 System > Logging

This section allows 4G/LTE Router to record the data and display the status of data.

5.2.1 Logging > Logging

- (1) Logging section provides you to control all logging records.
- (2) Users need to select **Apply** to confirm your settings.

System > Logging > Logging	
Item	Description
Mode	Turn on/off the logging configuration. Select from Disable or Enable. The default is Enable.
Remote Log	The logging messages send to remote log or not. Select from Disable or Enable. The default is Disable.
Log Server Address	When you choose “Enable” on Remote Log, you should input IP address to save and receive all logging data. (<i>Note:</i> This server should have installed Log software.)

5.2.2 Logging > Log

This section displays all data status.

- (1) You can choose Filter function to quickly search for your data.
- (2) When you click **Clear**, all of the data that displays on the interface will be totally cleared without any backup.
- (3) When you click **Refresh**, the system will update and display the latest data from your 4G/LTE Router.
- (4) When you click **Download Logs**, the system will download the latest data from your 4G/LTE Router.



The screenshot shows a web interface for logging. At the top, there is a blue header with a user icon and the word "Log". Below the header is a search bar labeled "filter". To the right of the search bar are three buttons: "Clear", "Refresh", and "Download Logs". Below the buttons is a table with the following headers: "#", "Date", "Group", "Module", and "Message".

System > Logging > Log	
Item	Description
Filter	Filter the required data quickly.
Date	Show the date of log for each logging data.
Group	Show the group of software functions.
Module	Show the module of group of software functions.
Message	Show the messages for each logging data.

5.3 System > Alarm

This section allows you to configure the alarm.

Note:

- (1) If you select **SNMP trap** in Alarm output, you need to set up SNMP trap configuration from Service SNMP.

System > Alarm	
Item	Description
Mode	Turn on/off the Alarm configuration. Select from Disable or Enable. The default is Enable.
Alarm Input	Select from SMS, VPN disconnect and WAN disconnect as input to trigger alarm. <ul style="list-style-type: none"> ● SMS: It means team members on selected week day can send SMS to the phone number of using SIM card to trigger alarm. ● VPN disconnect: All tunnels get disconnected then trigger alarm. ● WAN disconnect: All WAN connections get disconnected then trigger alarm.
Alarm Output	Select from SMS, SNMP trap and E-mail as alarm output.
Groups	Create your contact phone book for each group and edit your information for each user.
SMS/E-mail	Write your messages and the messages limit 150 English characters to deliver.

5.3.1 Alarm > Name Group

(1) How to create your group

- Name a group : Click **Group** for naming and the interface will show the group's name in the Group setting as below.


The screenshot illustrates the process of creating a group in the alarm system interface. It is divided into three parts:

- Top Left:** Shows the 'Groups' section with a 'Group' dropdown menu. A red box highlights the 'Group' dropdown and the 'SMS/E-mail' field. A 'Group name' input field is visible, with a red 'X' and a blue checkmark button.
- Top Right:** An arrow points to the 'Group' dropdown menu, which is now open, showing 'Office1' and a 'Create group' option. A red box highlights the dropdown menu.
- Bottom:** Shows the 'Group' table with columns for 'Name', 'SUN', 'MON', 'TUE', 'WED', 'THU', 'FRI', and 'SAT'. The 'Office1' group is listed in the 'Name' column. A red box highlights the 'Group' table.


An 'Apply' button is located at the bottom right of the interface.

5.3.2 Alarm > Edit User

(2) How to edit each user's information in every group

- Select your naming group and click add user button  to edit your user's information, including Name, Phone and E-mail.

The screenshot shows the 'Group' table in the alarm system interface. The table has columns for 'Name', 'SUN', 'MON', 'TUE', 'WED', 'THU', 'FRI', and 'SAT'. The 'Office1' group is listed in the 'Name' column. A red box highlights the 'Group' table. An 'Apply' button is located at the bottom right of the interface.

- After filling in your information for each row, chose your naming group and click  to submit your settings.

User
✕

Name

Phone

E-mail

Groups Office1

- After submitting your setting, the interface returns to Group window setting. Please click your naming group to show the user's information that you have edited.

Group

Name	SUN	MON	TUE	WED	THU	FRI	SAT
Office1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

User

All Users	Name	Phone	E-mail	Edit
Office1	test	+886912345678	test@test.com	

- You can click button to add the new user's information.

User

All Users	Name	Phone	E-mail	Edit
Office1	test	+886912345678	test@test.com	

5.4 System > Ethernet Ports

This section allows you to configure the Ethernet Ports.

Ethernet Ports

Status

LAN 1	100M Half
LAN 2	Off
LAN 3	Off
WAN	Off

Configurations

LAN 1	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable
LAN 2	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable
LAN 3	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable
WAN	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable

System > Ethernet Ports	
Item	Description
Status	Show the connectivity status of LAN and WAN.
Configurations	Select from Auto, 100M Full, 100M Half, 10M Full, 10M Half and Disable.

5.5 System > Client List

This section allows you to understand how many devices have been connected and their status from the router. There are two types, one is **DHCP Client** and the other is **Online**. The default is both types to show all status when the router is on DHCP Client and Online.

For **DHCP Client** type, the information shows IP address, MAC address, Hostname and the expiry time of IP (Start/End).

Client List

List Type DHCP Client Online

#	IP Address	MAC Address	Hostname	Start	End
1	192.168.1.2	20:cf:30:69:b9:ac	ASUS-K42-NB	2017/12/04 10:20:47	2017/12/04 15:20:47

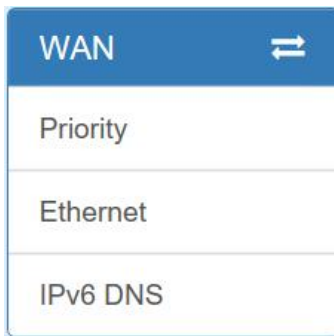
For **Online** type, the information shows IP address and MAC address when the client is online.

Client List		
List Type		
	<input type="checkbox"/> DHCP Client	<input checked="" type="checkbox"/> Online
#	IP Address	MAC Address
1	192.168.1.2	20:cf:30:69:b9:ac

System > Client List	
Item	Description
List Type	<ul style="list-style-type: none">● DHCP Client: List all clients' information when it is via DHCP.● Online: List the information when it is online.

6 Configuration > WAN

This section allows you to configure WAN, including Priority, LTE Config, Dual SIM, Ethernet and DNS.



6.1 WAN > Priority

You can set up the priority of WAN.

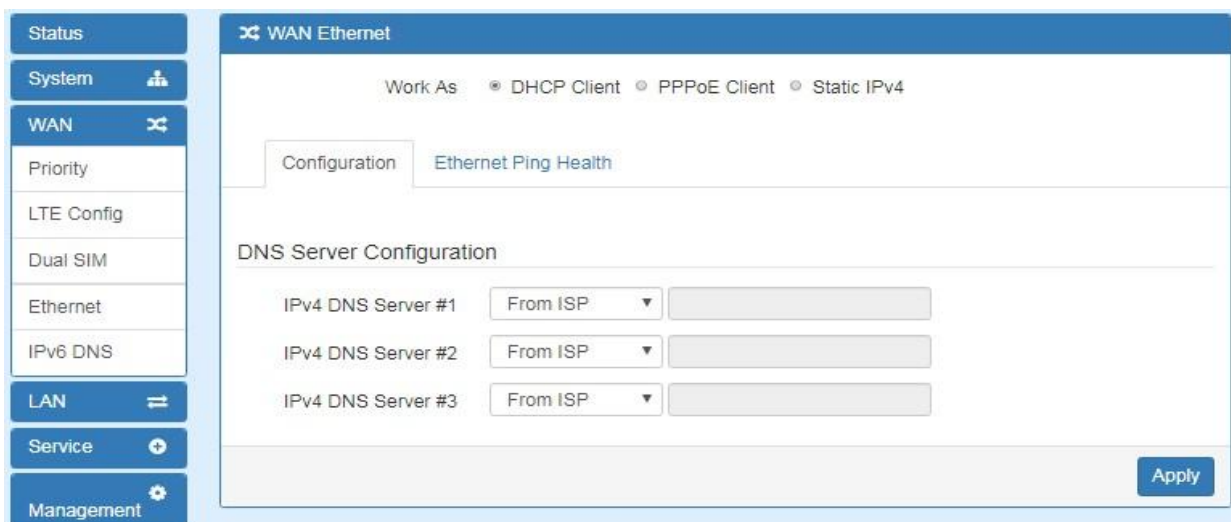


WAN > Priority	
Item	Description
Priority	<ul style="list-style-type: none">• Auto: WAN Ethernet is first priority and second priority is LTE. The default is Auto.• LTE Only: The priority is only LTE.• ETH Only: The priority is only Ethernet.

6.2 WAN > Ethernet

6.2.1 WAN Ethernet Configuration

This section provides three options, including **DHCP Client**, **PPPoE Client** and **Static IPv4**. The default is DHCP Client.



WAN > Ethernet	
Item	Description
WAN Ethernet	<p>There are three options to obtain the IP of WAN Ethernet.</p> <ul style="list-style-type: none"> ● DHCP Client: DHCP server-assigned IP address, netmask, gateway, and DNS. ● PPPoE Client: Your ISP will provide you with a username and password. This option is typically used for DSL services. ● Static IPv4: User-defined IP address, netmask, and gateway address.

When selecting “**DHCP Client**”, you can set up DNS Server Configuration.

For IPv4 DNS Server, it provides three options to set up and each option has provided with “From ISP”, “User Defined” and “None” to configure.

The screenshot shows the 'WAN Ethernet' configuration page. At the top, there are radio buttons for 'Work As' with options: 'DHCP Client' (selected), 'PPPoE Client', and 'Static IPv4'. Below this, there are two tabs: 'Configuration' (active) and 'Ethernet Ping Health'. The 'DNS Server Configuration' section contains three rows for 'IPv4 DNS Server #1', '#2', and '#3'. Each row has a dropdown menu with options 'From ISP', 'User Defined', and 'None', and an adjacent text input field. The 'From ISP' option is selected for all three servers. An 'Apply' button is located at the bottom right of the configuration area.

WAN > Ethernet	
Item	Description
<p>IPv4 DNS Server #1</p> <p>IPv4 DNS Server #2</p> <p>IPv4 DNS Server #3</p>	<ul style="list-style-type: none"> ● Each setting DNS Server has three options, including From ISP, User Defined and None. ● When you select From ISP, the IPv4 DNS server IP is obtained from ISP. ● When you select User Defined, the IPv4 DNS server IP is input by user.

When you select **PPPoE Client**, the interface shows the item of configuration to fill in your User Name and Password.

WAN Ethernet

Work As DHCP Client PPPoE Client Static IPv4

Configuration | Ethernet Ping Health

PPPoE Client Configuration

User Name

Password

Apply

When you select **Static IPv4**, the interface shows the information of configuration, including IP Address, IP Mask and Gateway Address.

WAN Ethernet

Work As DHCP Client PPPoE Client Static IPv4

Configuration | Ethernet Ping Health

Static IPv4 Configuration

IP Address

IP Mask

Gateway Address

DNS Server Configuration

IPv4 DNS Server #1

IPv4 DNS Server #2

IPv4 DNS Server #3

Apply

WAN > Ethernet	
Item	Description
Static IPv4 Configuration	
IP Address	Fill in the IP Address.
IP Mask	Fill in the IP Mask.
Gateway Address	Fill in Gateway Address.
DNS Server Configuration	
IPv4 DNS Server #1	The IPv4 DNS server IP is input by user.
IPv4 DNS Server #2	
IPv4 DNS Server #3	

6.2.2 Ethernet Ping Health

If you configure “WAN Priority” to “Auto” mode, the system would choose the cost effective connection first such as Ethernet. However in case the Ethernet connection exist but it is unable to access internet; you can enable “Ethernet Ping Health” and the system would switch to LTE connection and switch back whenever Ethernet is able to access internet again.

The screenshot shows the WAN Ethernet configuration interface. On the left is a navigation menu with options: Status, System, WAN (selected), Priority, LTE Config, Dual SIM, Ethernet, IPv6 DNS, LAN, Service, and Management. The main content area is titled 'WAN Ethernet' and includes a 'Work As' section with radio buttons for DHCP Client, PPPoE Client (selected), and Static IPv4. Below this is the 'Ethernet Ping Health' configuration section, which is currently selected. It features a radio button to toggle 'Ethernet Ping Health' between 'Disable' and 'Enable' (selected). An 'Interval' field is set to '10' with a note '(1 ~ 60 Seconds)'. There are four input fields for hosts: IPv4 Host 1 (www.google.com), IPv4 Host 2 (www.yahoo.com), IPv6 Host 1 (ipv6.google.com), and IPv6 Host 2 (www.ipv6.hinet.net). A 'Hint' section explains that with 'Wan Priority: Auto' and 'Ethernet ping health: Enable', the system will switch to LTE if the ping fails and back to Ethernet if it passes. An 'Apply' button is located at the bottom right.

WAN > Ethernet > Ethernet Ping Health	
Item	Description
Ethernet Ping Health	Select from Disable or Enable. The default is Enable.
Interval	The interval is from 1 to 60 seconds.
IPv4 Host 1	Input the address of IPv4 Host 1.
IPv4 Host 2	Input the address of IPv4 Host 2.
IPv6 Host 1	Input the address of IPv6 Host 1.
IPv6 Host 2	Input the address of IPv6 Host 2.
Hint	Show the usage descriptions.

In addition, you can check which WAN is actually using from “Status” page. The interface will be shown **check mark** (✓ symbol) on the connection title. For IPv6 address, the status will be displayed on LAN Ethernet Interface when IPv6 is using as WAN connection.

WAN LTE

Attr.	Current SIM	Backup SIM
SIM Card	SIM2	SIM1
Modem Status	Ready	Locked
Operator	Far EasTone	Chunghwa Telecom
Modem Access	FDD LTE	FDD LTE
IMSI	466011100041467	466924290307730
Phone Number		
Band	LTE BAND 3	LTE BAND 7
Channel ID	1550	3050
IPv4 Address	10.146.86.142	
IPv4 Mask	255.255.255.255	

WAN Ethernet		LAN Ethernet	
Attr.	Value	Attr.	Value
IPv4 Address	118.167.125.240	IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.255	IPv4 Mask	255.255.255.0
		IPv6 Address	2001:b011:7000:434::100

6.3 WAN > IPv6 DNS

This section allows you to set up IPv6 DNS Server Configuration.

IPv6 DNS

DNS Server Configuration

IPv6 DNS Server #1

IPv6 DNS Server #2

IPv6 DNS Server #3

For IPv6 DNS Server, it provides three options to set up and each option has provided with "From ISP", "User Defined" and "None" to configure.

IPv6 DNS

DNS Server Configuration

IPv6 DNS Server #1

IPv6 DNS Server #2

IPv6 DNS Server #3

WAN > IPv6 DNS	
Item	Description
DNS Server Configuration	
IPv6 DNS Server #1 IPv6 DNS Server #2 IPv6 DNS Server #3	<ul style="list-style-type: none"> • Each setting DNS Server has three options, including From ISP, User Defined and None. • When you select From ISP, the IPv6 DNS server IP is obtained from ISP. • When you select User Defined, the IPv6 DNS server IP is input by user.

7 Configuration > LTE

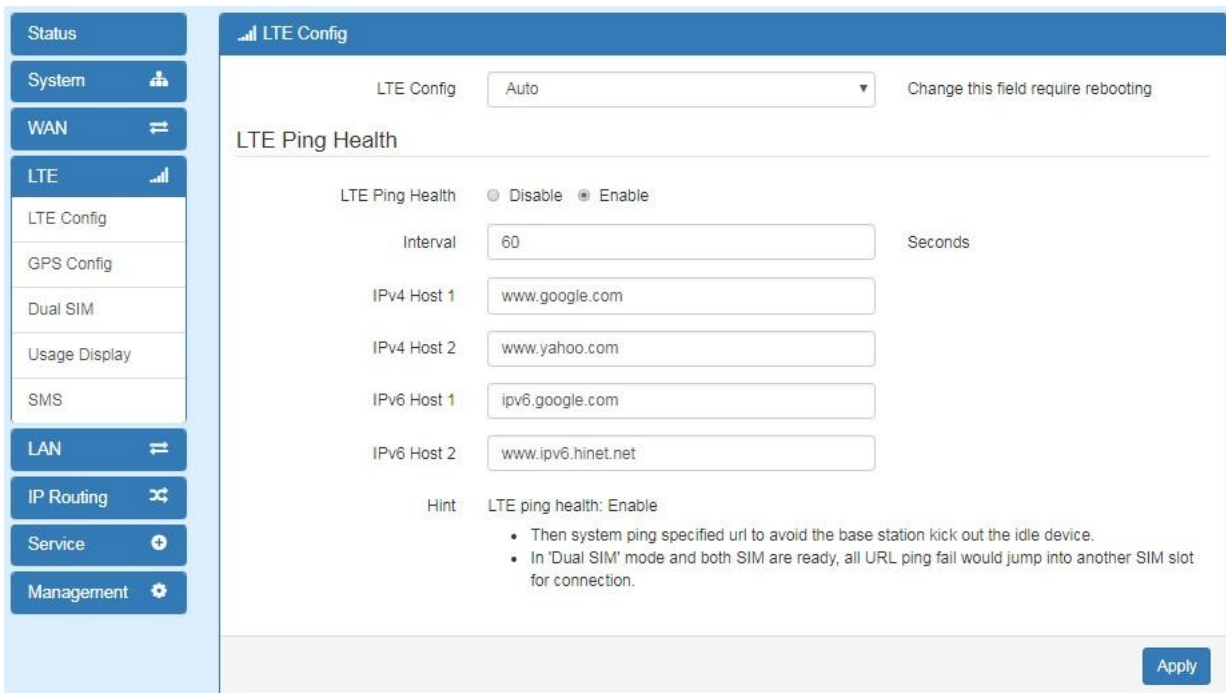
This section allows you to configure LTE Config, GPS Config, Dual SIM, Usage Display and SMS.



7.1 LTE > LTE Config

7.1.1 LTE Configuration

You can set up the LTE Configuration and LTE Ping Health.



For LTE Configuration, you can select from Auto, 4G Only, 3G Only or 2G Only.



LTE > LTE Config	
Item	Description
Auto	Automatically connect the possible band.
4G Only	Connect to 4G network only.
3G Only	Connect to 3G network only.
2G Only	Connect to 2G network only.

7.1.2 LTE Ping Health

For LTE connection, you can enable “**LTE Ping Health**” to keep alive to avoid base station kicking out the device in idle time.

Note: In 'Dual SIM' mode and both SIM are ready, all URL ping fail would jump into another SIM slot for connection.

The screenshot shows the 'LTE Config' interface. At the top, there is a dropdown menu for 'LTE Config' set to 'Auto', with a note 'Change this field require rebooting'. Below this is the 'LTE Ping Health' section. It features a radio button selection for 'LTE Ping Health' with 'Enable' selected. There are input fields for 'Interval' (60), 'IPv4 Host 1' (www.google.com), 'IPv4 Host 2' (www.yahoo.com), 'IPv6 Host 1' (ipv6.google.com), and 'IPv6 Host 2' (www.ipv6.hinet.net). A 'Hint' section provides additional information: 'LTE ping health: Enable' followed by two bullet points explaining the feature's purpose and behavior in Dual SIM mode. An 'Apply' button is located at the bottom right.

LTE > LTE Config > LTE Ping Health	
Item	Description
LTE Ping Health	Select from Disable or Enable.
Interval	Input the interval seconds of ping.
IPv4 Host 1	Input the address of IPv4 Host 1.
IPv4 Host 2	Input the address of IPv4 Host 2.
IPv6 Host 1	Input the address of IPv6 Host 1.
IPv6 Host 2	Input the address of IPv6 Host 2.
Hint	Show the usage descriptions.

7.2 LTE > Dual SIM

This section allows you to understand the status of connectivity for Dual SIM, SIM1 and SIM2. The **Used SIM** item has three options and the default is on Dual SIM when first connection. The **Connect Retry Number** field can set up the re-connecting time if your one of the SIM cards on Dual SIM mode can't connect successfully. The default of Connect Retry Number is 3 minutes.



The screenshot shows the 'Dual SIM' settings page with the 'Connect Policy' section. The 'Current SIM Card' is set to SIM1, with a 'Disconnect' button next to it. The 'Disable Roaming' option is set to 'Yes'. The 'Used SIM' option is set to 'Dual SIM'. The 'SIM Priority' option is set to 'SIM1'. The 'Roaming Switch' option is checked, with the text 'Switch to another SIM when roaming is detected'. The 'Connect Retry Number' is set to 3, with a note '(1 ~ 100) * 60 seconds'.

For **Roaming Switch**, it means Switch to another SIM when roaming is detected. System will switch SIM slot when current SIM is in roaming state and another SIM slot is in READY state.

If you have selected either SIM1 or SIM2 for the **Used SIM** to connect, the **Roaming Switch** and **Connect Retry Number** would not to be shown in the interface.



The screenshot shows the 'Dual SIM' settings page with the 'Connect Policy' section. The 'Current SIM Card' is set to SIM1, with a 'Disconnect' button next to it. The 'Disable Roaming' option is set to 'Yes'. The 'Used SIM' option is set to 'SIM1'. The 'Roaming Switch' and 'Connect Retry Number' options are not visible in this configuration.

You can set up the SIM cards, SIM1 Configurations or SIM2 Configurations.

- **SIM PIN:** If you has configured SIM PIN code into SIM card, please type SIM PIN code in Dual SIM configuration to make unlock successfully.
- **SIM PUK:** If you has typed wrong SIM PIN code and retried more than 3 times, the SIM Card will become the blocked mode. In this case, you have to type PUK and new SIM code to unlock SIM Card.

Connect Policy

Current SIM Card SIM1 [Disconnect](#)

Disable Roaming No Yes

Used SIM Dual SIM SIM1 SIM2

SIM Priority Auto SIM1 SIM2

Roaming Switch Switch to another SIM when roaming is detected

Connect Retry Number (1 ~ 100) * 60 seconds

SIM1 Configurations SIM2 Configurations

Status Ready

SIM PIN	<input type="text"/>
Confirmed SIM PIN	<input type="text"/>
SIM PUK	<input type="text"/>
Confirmed SIM PUK	<input type="text"/>
APN	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Change SIM PIN	Change

Data Limitation

Already Used Data (MB) 2

Mode Disable Enable

Max Data Limitation (MB)

Monthly Reset Date: Hours: Minutes: Seconds:

Now Time Date: 1 Hours: 10 Minutes: 15 Seconds: 21

[Apply](#)

- **Change SIM PIN** : If you want to change SIM PIN code, you can click **Change** button and type old SIM PIN code and new SIM PIN code. Please aware not to exceed the retry number (PIN remaining number and PUN remaining number).

Change SIM PIN

Change

Old PIN

New PIN

PIN Remaining Number 0

PUK Remaining Number 0

Apply

Note:

The interface will be shown the tick symbol at the same time when each SIM Card has been connected.

Dual SIM

Connect Policy

Current SIM Card SIM1 [Disconnect](#)

Disable Roaming Disable Enable

Used SIM Dual SIM SIM1 SIM2

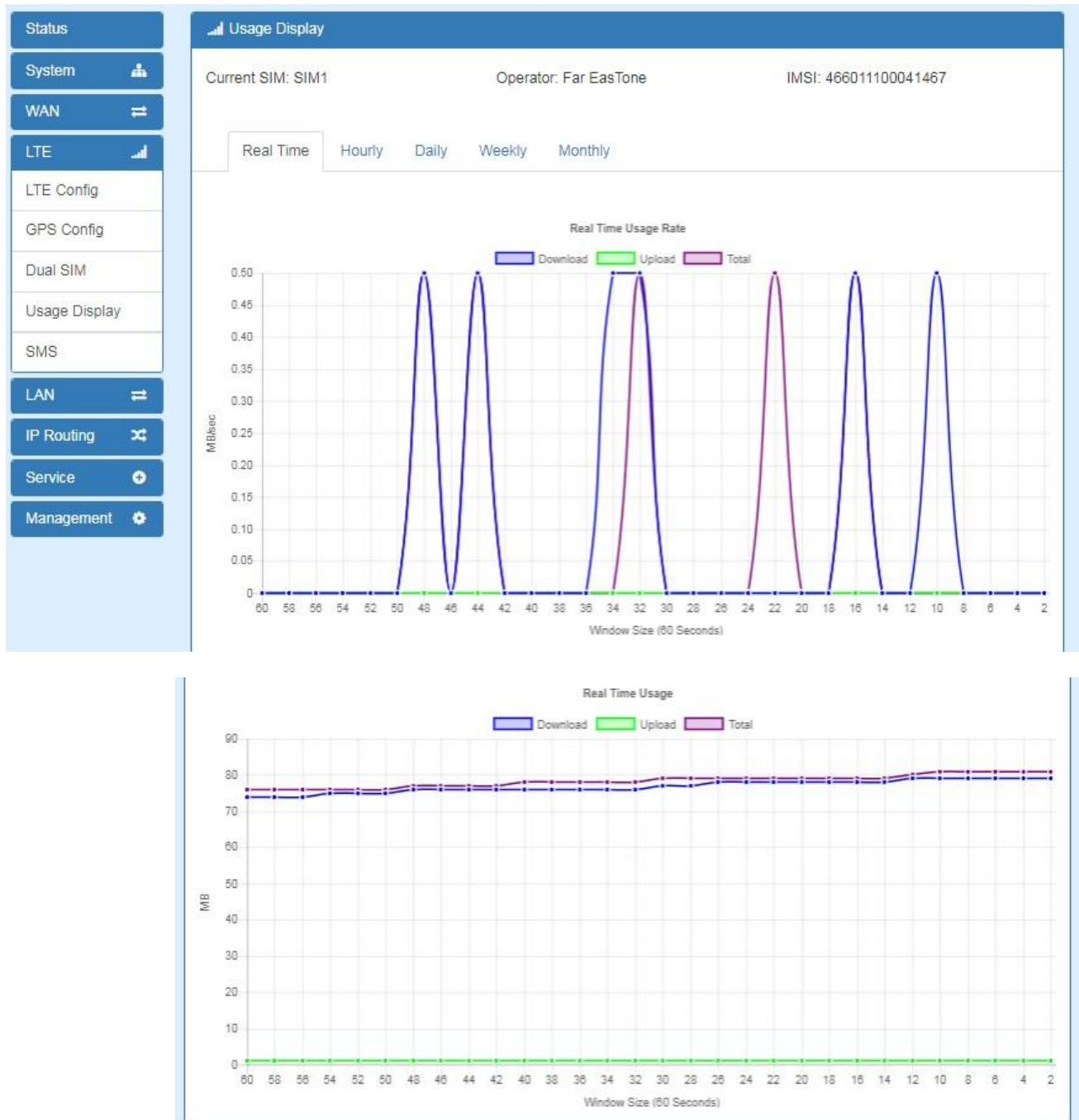
SIM1 Configurations SIM2 Configurations

Status Ready

LTE > Dual SIM	
Item	Description
Connect Policy	
Current SIM Card	Display which SIM slot is using.
Status of SIM Card Connectivity	<ul style="list-style-type: none"> ● Connect: After manually disconnect, user can only click Connect button to get connection or reboot the device to make it automatically connect. ● Disconnect: If there is one SIM slot get connection, the Disconnect button appear. After manually click Disconnect, the system would not automatically get connection until next reboot.
Disable Roaming	<ul style="list-style-type: none"> ● Disable: SIM gets connection even it is in roaming state. ● Enable: SIM would not get connection when in roaming state.
Used SIM	Three options to show SIM Card's used status, including Dual SIM, SIM1 and SIM2.
SIM Priority	Three options to set the priority for SIM Card, including Auto, SIM1 and SIM2. To set up the first link SIM slot from Dual SIM mode with two SIM cards.
Roaming Switch	Switch to another SIM when roaming is detected. System will switch SIM slot when current SIM is in roaming state and another SIM slot is in READY state.
Connect Retry Number	Entry the time when SIM card starts to activate. This option is only for Dual SIM mode.
SIM1 Configurations or SIM2 Configurations	
Status	Display the status of Dual SIM.
SIM PIN	Configure PIN code to unlock SIM PIN.
Confirmed SIM PIN	Confirm PIN code.
SIM PUK	Fill in PUK to unlock SIM Card after typing more than 3 times.
Confirmed SIM PUK	Confirm SIM PUK.
APN	APN can be input by user or the system will search from internal database if APN is blank.
Username	The username can be input by user or the system will search from internal database if the username is blank.
Password	The password can be input by user or the system will search from internal database if the password is blank.
Confirm Password	Fill in your changed password.
Change SIM PIN	Change your old SIM PIN code into new SIM PIN code.
Data Limitation	
Mode	Turn on/off the Data Limitation to disable or enable.
Already Used Data (MB)	Display current used throughput since last reset.
Max Data Limitation (MB)	Configure max throughput.
Monthly Reset	Set up the reset time during the month.
Now Time	Show the current time of system.

7.3 LTE > Usage Display

This section shows the status of **current SIM card**, **operator**, **IMSI** and the charts for **Real Time**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.



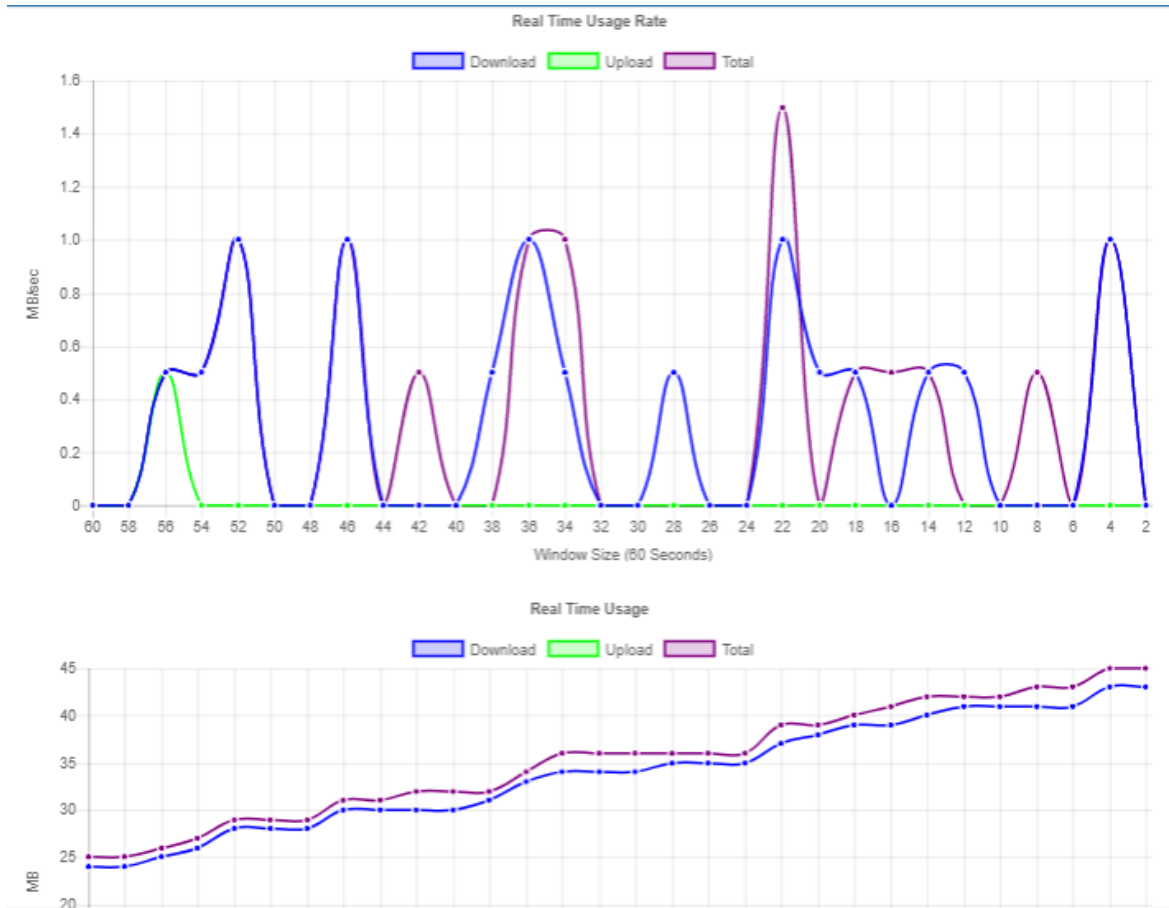
(1) Real-Time Usage:

- **Real-Time Usage Rate:**

It displays real-time Download/Upload/Total MB per seconds for current using SIM card and the view window size is 60 seconds.

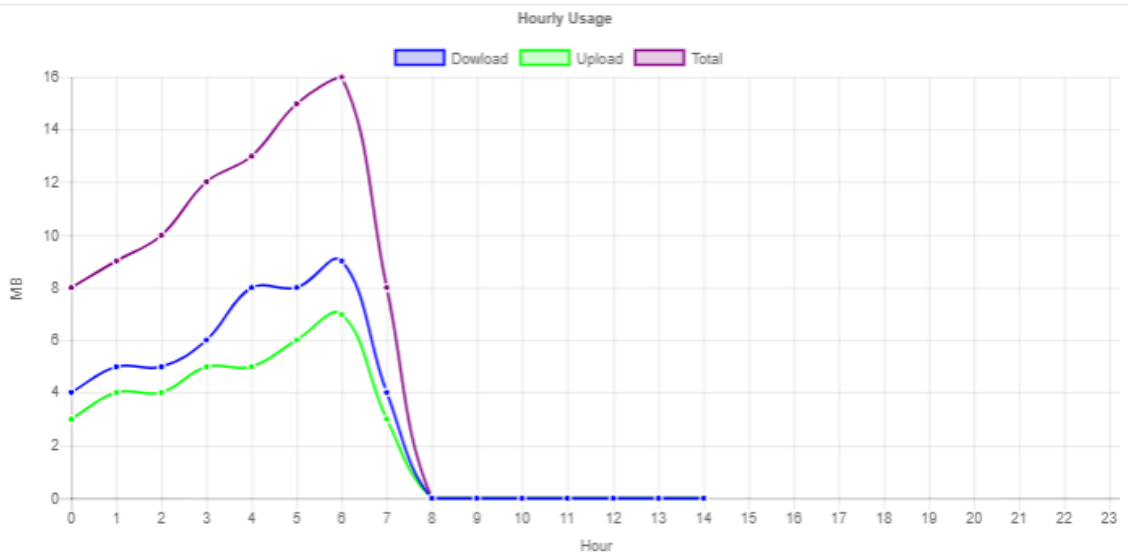
- **Real-Time Usage:**

It displays accumulated real-time Download/Upload/Total MB per seconds for current using SIM card and the view window size is 60 seconds.



(2) Hourly Usage:

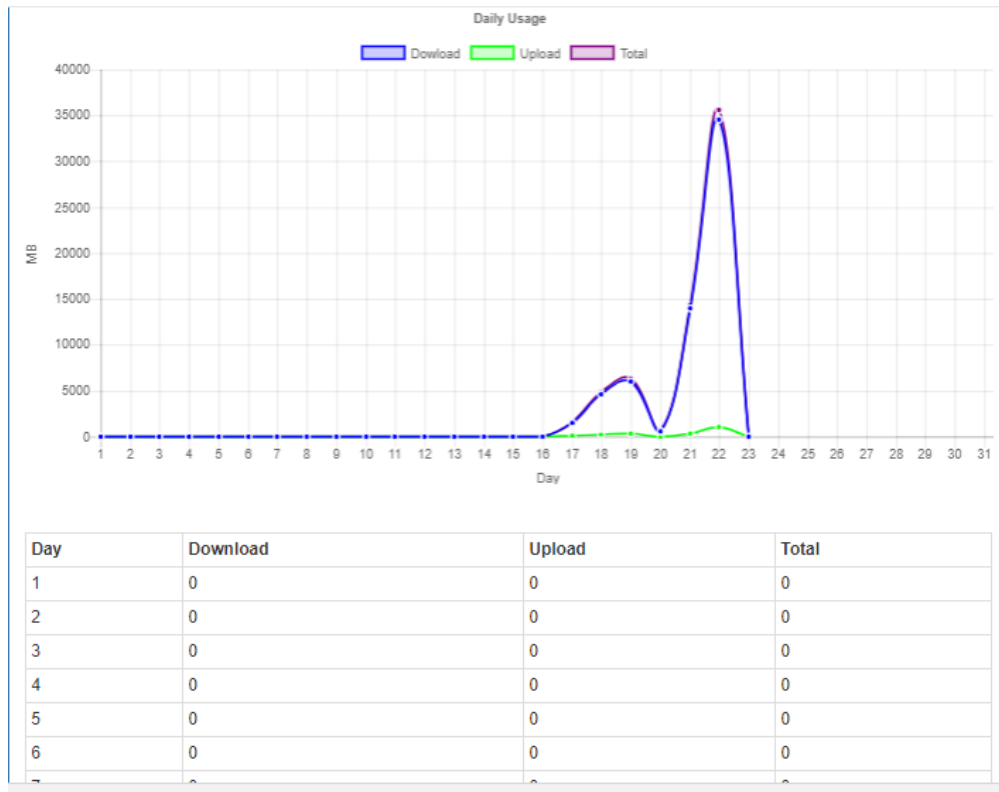
It displays Download/Upload/Total MB per hour in one day for current using SIM card and the view window size is 24 hours.



Hour	Download	Upload	Total
0	4	3	8
1	5	4	9
2	5	4	10
3	6	5	12
4	8	5	13
5	8	6	15
6	9	7	16
7	4	3	8
8	0	0	0
9	0	0	0
10	0	0	0
11	0	0	0
12	0	0	0
13	0	0	0
14	0	0	0
15	0	0	0
16	0	0	0
17	0	0	0
18	0	0	0
19	0	0	0
20	0	0	0
21	0	0	0
22	0	0	0
23	0	0	0

(3) Daily Usage:

It displays Download/Upload/Total MB per day in one month for current using SIM card and the view window size is 31 days.



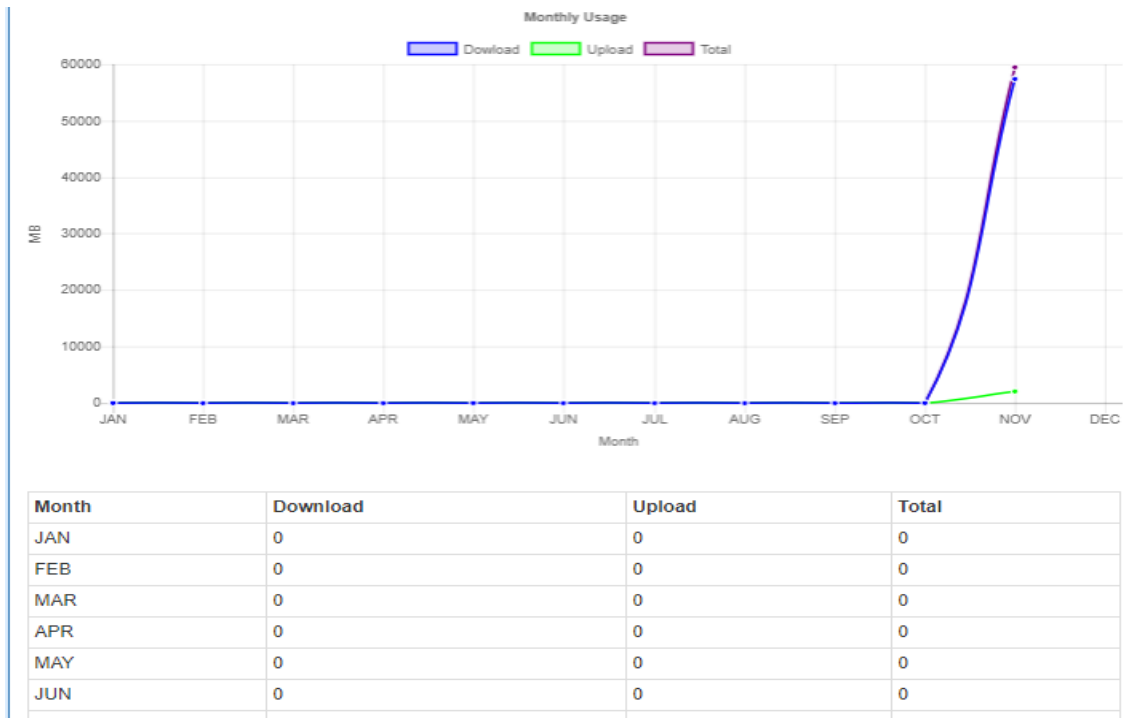
(4) Weekly Usage:

It displays Download/Upload/Total MB per day in one week for current using SIM card and the view window size is 7 days.



(5) Monthly Usage:

It displays Download/Upload/Total MB per month in one year for current using SIM card and the view window size is 12 months.



7.4 LTE > SMS


This section provides two settings, one is **SMS Action** and the other is **View SMS**.

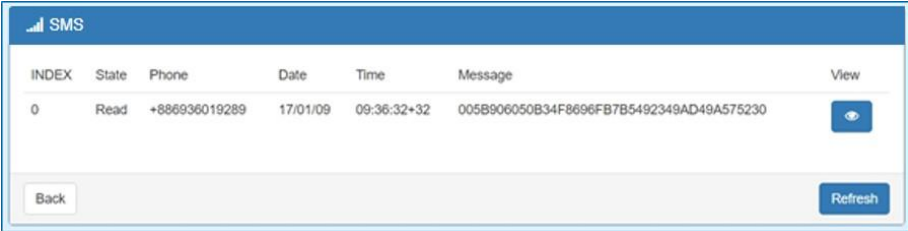
- (1) When enabling **SMS Action**, it allows you by sending key words SMS to trigger device setting/action/query status.

The screenshot shows the 'SMS Action' configuration page. The 'Mode' is set to 'Enable'. Under 'Actions and Keywords Setup', the following keywords are defined:


- Reboot: ##SMS REBOOT##
- Disconnect LTE: ##MOBILE DISCONNECT##
- Connect LTE: ##MOBILE CONNECT##
- Disble OpenVPN: ##OPENVPN DISABLE##
- Enable OpenVPN: ##OPENVPN ENABLE##
- Disable IPsec: ##IPSEC DISABLE##
- Enable IPsec: ##IPSEC ENABLE##
- Query Mobile Status: ##MOBILE STATUS##

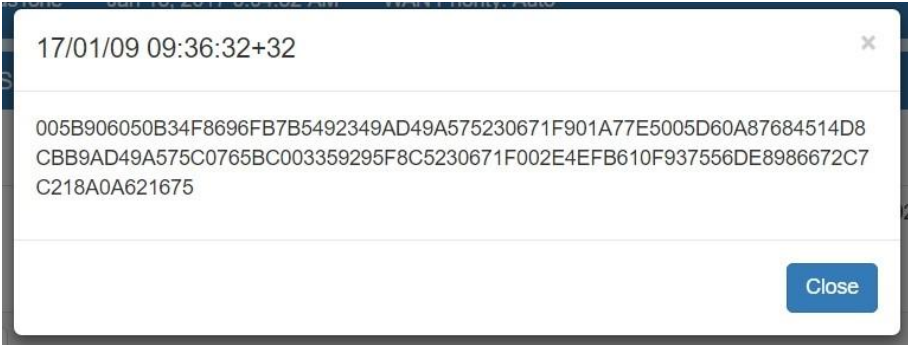
An 'Apply' button is located at the bottom right of the configuration area.

(2) For **View SMS**, this section allows you to review the information of SMS that you have received, including the state, phone and date and time. You can click  **view button** to review all messages.



The screenshot shows a table with the following columns: INDEX, State, Phone, Date, Time, Message, and View. A single row of data is visible, and a 'View' button with an eye icon is located to the right of the message content. At the bottom of the table, there are 'Back' and 'Refresh' buttons.

INDEX	State	Phone	Date	Time	Message	View
0	Read	+886936019289	17/01/09	09:36:32+32	005B906050B34F8696FB7B5492349AD49A575230	



The screenshot shows a detailed view of an SMS. At the top, the date and time '17/01/09 09:36:32+32' are displayed. Below this, the full message content is shown as a long alphanumeric string. A 'Close' button is located at the bottom right of the view.

17/01/09 09:36:32+32

005B906050B34F8696FB7B5492349AD49A575230671F901A77E5005D60A87684514D8
CBB9AD49A575C0765BC003359295F8C5230671F002E4EFB610F937556DE8986672C7
C218A0A621675

Close

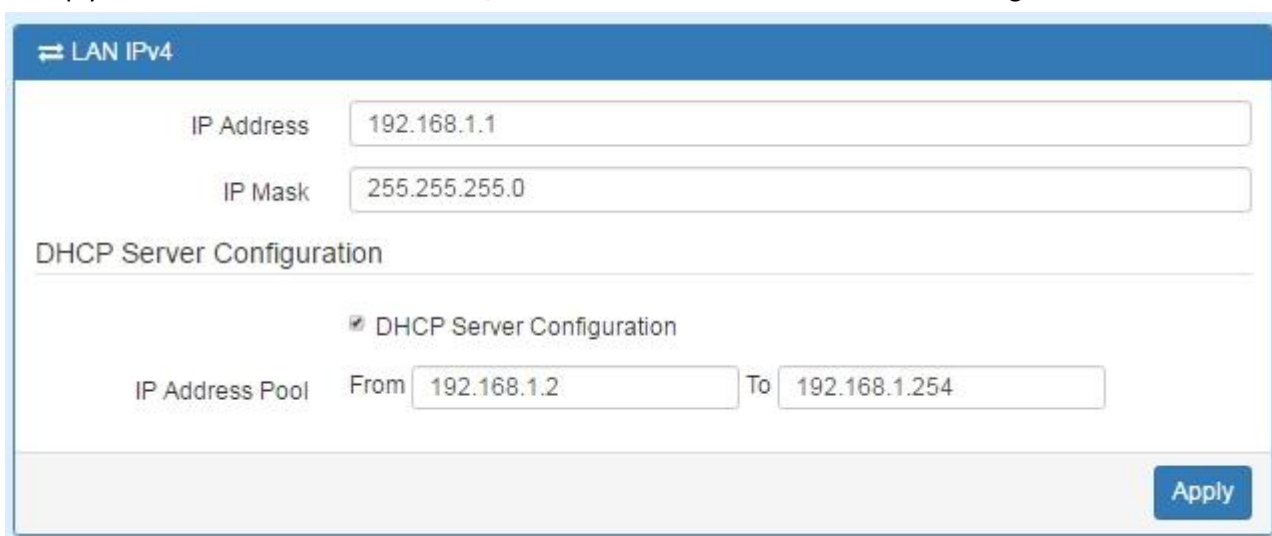
8 Configuration > LAN

This section allows you to configure LAN IPv4, LAN IPv6, VLAN and Subnet.



8.1 LAN > IPv4

Set up your IP Address and IP Mask. Also, fill in the information of DHCP Server Configuration.

A screenshot of a web-based configuration interface for LAN IPv4. The page has a blue header with a double arrow icon and the text 'LAN IPv4'. Below the header, there are two input fields: 'IP Address' with the value '192.168.1.1' and 'IP Mask' with the value '255.255.255.0'. Below these is a section titled 'DHCP Server Configuration' with a checked checkbox labeled 'DHCP Server Configuration'. Underneath, there is an 'IP Address Pool' section with 'From' and 'To' input fields containing '192.168.1.2' and '192.168.1.254' respectively. A blue 'Apply' button is located in the bottom right corner.

LAN > IPv4	
Item	Description
LAN IPv4	<ul style="list-style-type: none">• IP Address:192.168.1.1• IP Mask:255.255.255.0 Both of them are default, you can change them according to your local IP Address and IP Mask.
DHCP Server Configuration	<ul style="list-style-type: none">• Turn on/off DHCP Server Configuration.• Enable to make router can lease IP address to DHCP clients which connect to LAN.
IP Address Pool	<ul style="list-style-type: none">• Define the beginning and the end of the pool of IP addresses which will lease to DHCP clients.

8.2 LAN > IPv6

Select your type of IPv6, which shows **Delegate Prefix from WAN** or **Static**, and then set up DHCP Server Configuration, including Address Assign, DNS Assign and DNS Server.

LAN > IPv6	
Item	Description
LAN IPv6	<ul style="list-style-type: none"> This section provides two types, including Delegate Prefix from WAN and Static. Static Address: You need to input the static address when you select the static type.
Delegate Prefix from WAN	<ul style="list-style-type: none"> Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	<ul style="list-style-type: none"> Select this option to configure a fixed IPv6 address for the 4G/LTE Router's LAN IPv6 address.
Address Assign Setup	Select how you obtain an IPv6 address: <ul style="list-style-type: none"> Stateless: The 4G/LTE Router uses IPv6 stateless auto configuration. RADVD (Router Advertisement Daemon) is enabled to have the 4G/LTE Router send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 clients. Stateful: The 4G/LTE Router uses IPv6 stateful auto configuration. The LAN IPv6 clients can obtain IPv6 addresses through DHCPv6.

8.3 LAN > VLAN

This section allows you to set up VLAN that provides a network segmentation system to distinguish the LAN clients and separate them into different LAN subnet for enhancing security and controlling traffic.

First, the **VLAN Mode** allows you to select **Off** or **Tag Base (802.1p)**.

When VLAN Mode is set to **Tag Base**, the VLAN setting window will appear as shown below.

For each row, the settings can be enabled or disabled by checkbox and select the **Subnet** and the **VLAN ID (VID)**. The **Subnet** sets up the IP address and IP mask for the router so this router can communicate with the third party by this IP address and IP mask on this VLAN. (**Note:** The NET1 can't remove it and fixes in the first row.)

VLAN

Mode Off Tag Base

Enable	Subnet	VID
<input checked="" type="checkbox"/>	NET1	1
<input type="checkbox"/>	NET2	2
<input type="checkbox"/>	NET3	3
<input type="checkbox"/>	NET4	4
<input type="checkbox"/>	NET5	5
<input type="checkbox"/>	NET6	6
<input type="checkbox"/>	NET7	7
<input type="checkbox"/>	NET8	8

Apply

Furthermore, the **Subnet** provides DHCP Server function to allow the third party for the same VLAN to get IP address and IP mask. Therefore, you do not need to configure manually.

(**Note:** The subnet information will show the Subnet window from the LAN catalogue.)

Status

System

WAN

LTE

LAN

IPv4

IPv6

VLAN

Subnet

Edit Subnet NET3

IP Address: 192.168.3.1

IP Mask: 255.255.255.0

DHCP Server Configuration

DHCP Server Configuration

IP Address Pool: From 192.168.3.2 To 192.168.3.254

Save

LAN > VLAN	
Item	Description
Mode	<ul style="list-style-type: none"> The VLAN mode is Off or Tag Base (802.1p VLAN).
Enable	<ul style="list-style-type: none"> The assigned row of setting are enabled.
Subnet	<ul style="list-style-type: none"> The subnet provides IP address and IP mask for the router.
VID	<ul style="list-style-type: none"> The VLAN ID range is from 1 to 4094.

8.4 LAN > Subnet

This section allows you to get the information of IP Address and IP Mask and edit for the Subnets from DHCP Server Configuration.

Name	IP Address	IP Mask	Edit
NET2	192.168.2.1	255.255.255.0	
NET3	192.168.3.1	255.255.255.0	
NET4	192.168.4.1	255.255.255.0	
NET5	192.168.5.1	255.255.255.0	
NET6	192.168.6.1	255.255.255.0	
NET7	192.168.7.1	255.255.255.0	
NET8	192.168.8.1	255.255.255.0	

Note: Subnet **NET1** is the default IPv4 LAN, go IPv4 for configuration.

Apply

This **Subnet** setting is the same with LAN->IPv4 setting and follows with Tag Base Mode of VLAN to enable the function.

Name	IP Address	IP Mask	Edit
NET2	192.168.2.1	255.255.255.0	
NET3	192.168.3.1	255.255.255.0	
NET4	192.168.4.1	255.255.255.0	
NET5	192.168.5.1	255.255.255.0	
NET6	192.168.6.1	255.255.255.0	
NET7	192.168.7.1	255.255.255.0	
NET8	192.168.8.1	255.255.255.0	

Note: Subnet **NET1** is the default IPv4 LAN, go IPv4 for configuration.

Apply

Edit Subnet NET2

IP Address

IP Mask

DHCP Server Configuration

DHCP Server Configuration

IP Address Pool From To

Save

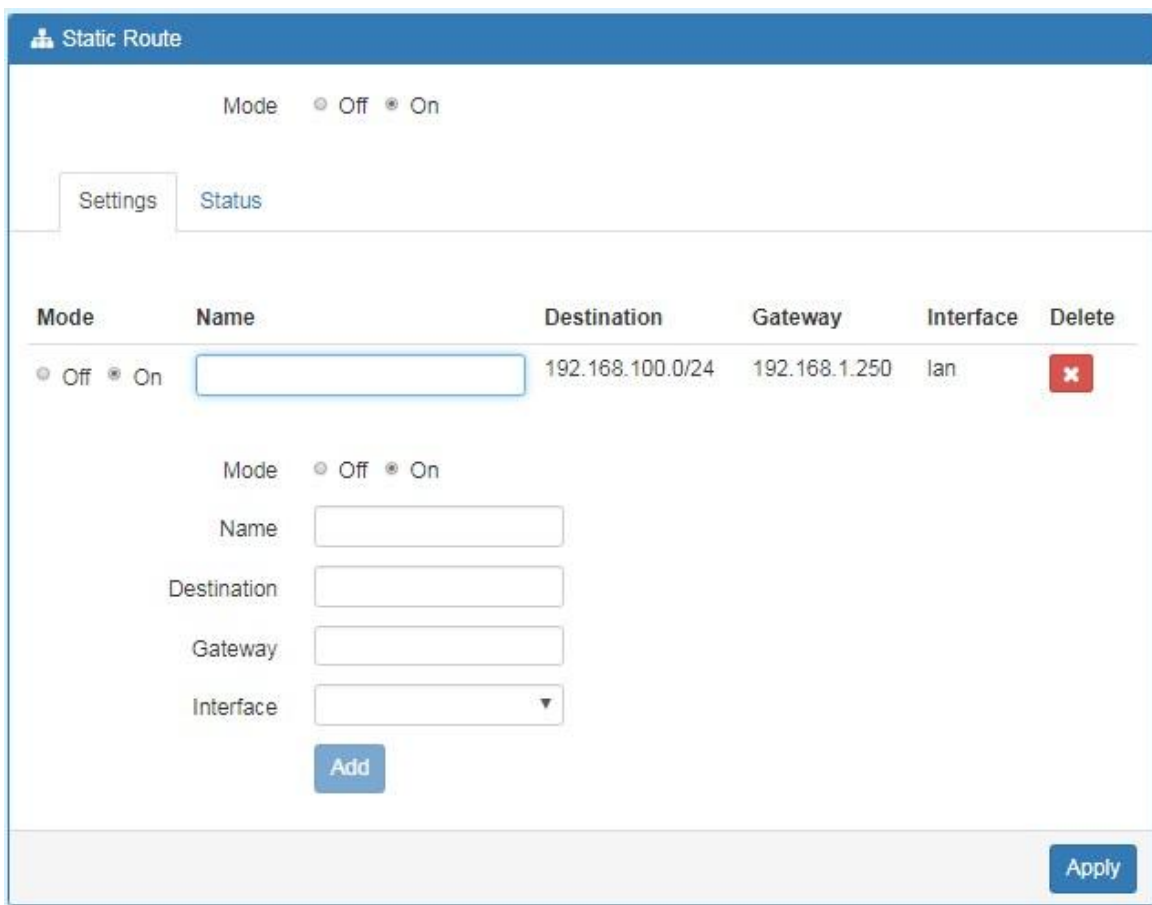
9 IP Routing

This section allows you to configure the Static Route and RIP.




9.1 IP Routing > Static Route

This section allows you to configure the Static Route. A static route is a pre-determined path that network information must follow to reach a specific host or network.



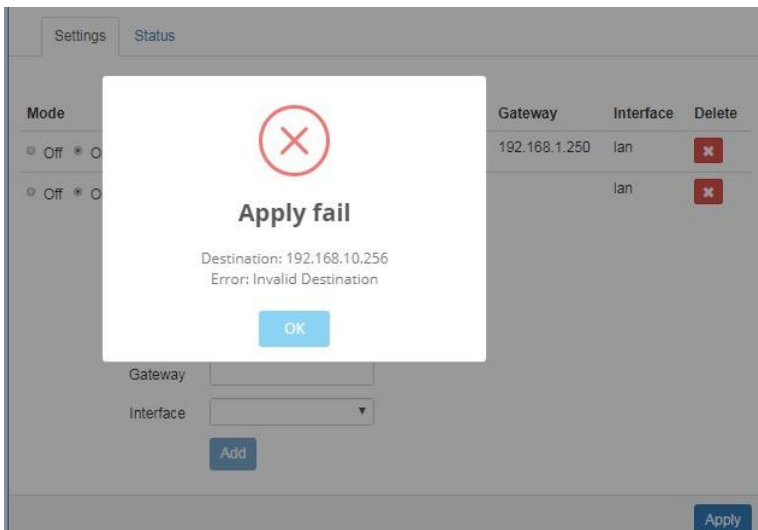
The "Static Route" configuration interface includes a "Mode" selector (Off/On), tabs for "Settings" and "Status", and a table of existing routes. Below the table are input fields for Name, Destination, Gateway, and Interface, along with an "Add" button and an "Apply" button at the bottom right.

Mode	Name	Destination	Gateway	Interface	Delete
<input type="radio"/> Off <input checked="" type="radio"/> On	<input type="text"/>	192.168.100.0/24	192.168.1.250	lan	

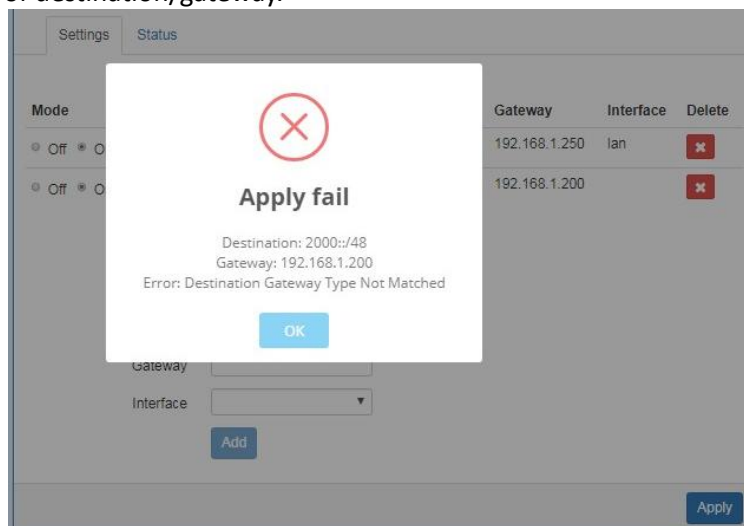
IP Routing > Static Route	
Item	Description
Mode	The setting is for full network. Select from Off or On.
Settings	
Mode	The setting is for the specific network. Select from Off or On.
Name	Set up each name for your running host or network.
Destination	Fill in the destination of a specific subnet or IP from network.
Gateway	Fill in the gateway address of your router.
Interface	Select the interface from LAN or Ethernet.

Note:

- The destination field is required to fill in. The format of destination is IPv4 or IPv6.
- The address of gateway or the type of interface can be chosen one or both to fill in the field.
- There are two fail situations when you fill in the incorrect type for the field.
 - (1) Input the invalid format of destination. The interface is shown in **Apply fail** to notice.



- (2) Input the IP address of destination/gateway from IPv4 and IPv6 at the same time. The interface is shown in **Apply fail** to notice. You should select either IPv4 or IPv6 as the address of destination/gateway.



The status tab shows the information from the settings of static route.

Static Route

Mode Off On

Settings Status

Destination	Gateway	Interface	Protocol
192.168.1.0/24		lan	kernel
192.168.100.0/24	192.168.1.250	lan	static
fe80::/64		eth0	kernel
fe80::/64		lan	kernel

Apply

IP Routing > Static Route	
Item	Description
Mode	The setting is open for full network. Select from Off or On.
Status	
Destination	Show the status of destination from the setting section.
Gateway	Show the status of gateway from the setting section.
Interface	Show the status of interface from the setting section.
Protocol	Show the status of protocol from the setting section.

9.2 IP Routing > RIP

This section allows you to configure RIP and select the mode from Disable or Enable. The default is Disable.

Note:

RIP (Routing Information Protocol, RFC 2453) is an Interior Gateway Protocol (IGP) and is commonly used in internal networks. It allows a router to exchange its routing information automatically with other routers, and allows it to dynamically adjust its routing tables and adapt to changes in the network.

IP Routing > RIP > Interfaces	
Item	Description
Interfaces	
Mode	Select from Off or On to use or not to use the RIP function in the interface.
Interface	Select from eth1(WAN Ethernet) or LAN .
Authentication	Select from none or md5 to approve authentication. Note: Please offer Key and Key ID when you select md5 to use HMAC-MD5.
Key	The key used for authentication (maxlength=16).
Key ID	The ID of the key used for authentication (1-255).
Passive	Select from Off or On to send out or not to send out RIP packets on this interface.

9.3 IP Routing > OSPF

This section allows you to set up **OSPF** with three sub configurations, including General, Interfaces and Networks configuration.

The screenshot shows the OSPF configuration page with a sidebar on the left containing menu items: Status, System, WAN, LTE, LAN, IP Routing (selected), Static Route, RIP, OSPF, BGP, Service, and Management. The main content area is titled 'OSPF' and has three tabs: General, Interfaces, and Networks. The 'General' tab is active and contains the following settings:

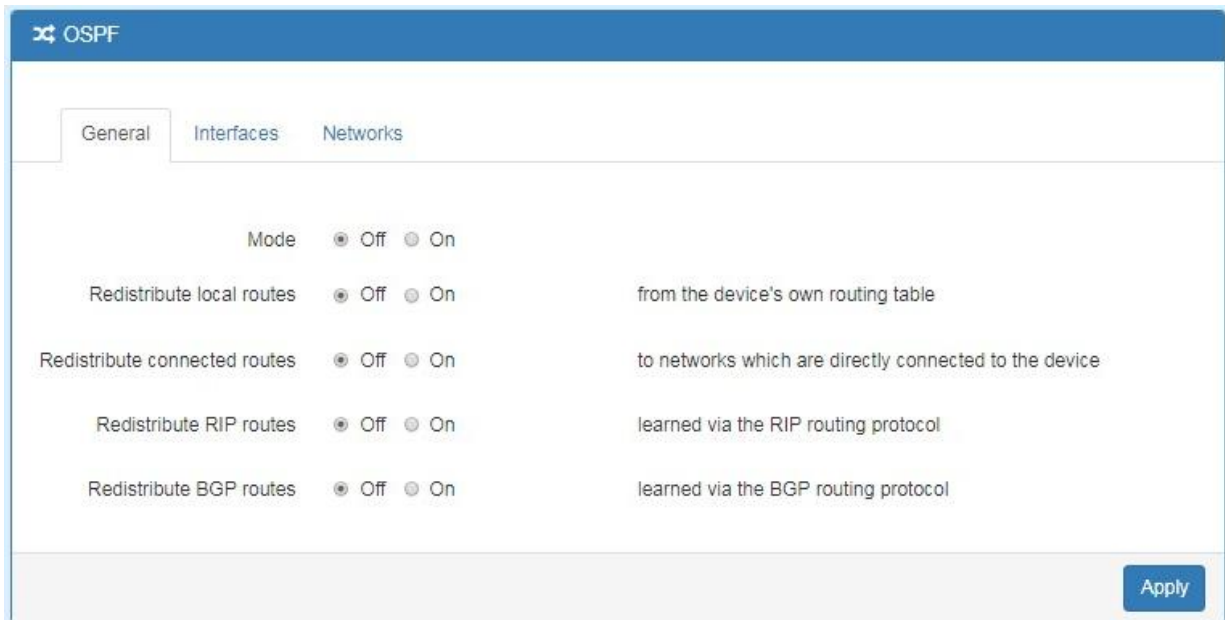
- Mode: Off On
- Redistribute local routes: Off On (from the device's own routing table)
- Redistribute connected routes: Off On (to networks which are directly connected to the device)
- Redistribute RIP routes: Off On (learned via the RIP routing protocol)
- Redistribute BGP routes: Off On (learned via the BGP routing protocol)

An 'Apply' button is located at the bottom right of the configuration area.

(1) General Configuration

You can have these settings for General configuration.

- Mode
- Redistribute local routes
- Redistribute connected routes
- Redistribute RIP routes
- Redistribute BGP routes



IP Routing > OSPF > General	
Item	Description
General	
Mode	<ul style="list-style-type: none"> ● Off: OSPF function is off. ● On: OSPF function is on.
Redistribute local routes	<ul style="list-style-type: none"> ● Off: Not redistribute local routes from the device's own routing table. ● On: Redistribute local routes from the device's own routing table.
Redistribute connected routes	<ul style="list-style-type: none"> ● Off: Not redistribute connected routes to networks which are directly connected to the device. ● On: Redistribute connected routes to networks which are directly connected to the device.
Redistribute RIP routes	<ul style="list-style-type: none"> ● Off: Not redistribute RIP routes learned via the RIP routing protocol. ● On: Redistribute RIP routes learned via the RIP routing protocol.
Redistribute BGP routes	<ul style="list-style-type: none"> ● Off: Not redistribute BGP routes learned via the RIP routing protocol. ● On: Redistribute BGP routes learned via the RIP routing protocol.

(2) Interfaces Configuration

There are 2 parts for OSPF Interfaces configuration.

- OSPF Interfaces Summary
 - Click **Edit** button to edit the existed interface.
 - Click **Delete** button to delete the existed interface.
- Add/Edit OSPF Interface

Note: This interface can be added at maximum is 2.

OSPF

General Interfaces Networks

								Summary	
#	Mode	Interface	Authentication	Key	Key ID	Cost	Passive	Edit	Delete
1	on	eth1	none	--	--	0	off		

Add OSPF Interface Add/Edit

Mode Off On

Interface

Authentication

Key The key used for authentication (maxlength=16)

Key ID The ID of the key used for authentication (1-255)

Cost The cost for sending packets via this interface (0: OSPF defaults)

Passive Off On Do not send out OSPF packets on this interface

IP Routing > OSPF > Interfaces	
Item	Description
Interfaces	
Mode	Select from Off or On to use or not to use the OSPF function in the interface.
Interface	Select from eth1(WAN Ethernet) or LAN .
Authentication	Select from none or md5 to approve authentication. Note: Please offer Key and Key ID when you select md5 to use HMAC-MD5.
Key	The key used for authentication (maxlength=16).
Key ID	The ID of the key used for authentication (1-255).
Cost	The cost for sending packets via this interface (0: OSPF defaults).
Passive	Select from Off or On to send out or not to send out OSPF packets on this interface.

(3) Networks Configuration

There are 2 parts for OSPF Networks configuration.

- OSPF Networks Summary
You can edit and delete the existed OSPF networks.
- OSPF Networks Add/Edit

This sub configuration is used to configure all the networks, the maximum is 2.

IP Routing > OSPF > Networks	
Item	Description
Networks	
Mode	Select from Off or On to enable the network setting.
Prefix	Set Prefix of the network
Prefix Length	Set Length of the prefix
Area	Routing area to which this interface belongs (0-65535, 0 means backbone)

9.4 IP Routing > BGP

This section allows you to set up **BGP** with three sub configurations, including General, Neighbors and Networks configuration.

(1) General Configuration

IP Routing > BGP > General	
Item	Description
General	
Mode	<ul style="list-style-type: none"> ● Off: BGP function is off. ● On: BGP function is on.
AS Number	The number of the autonomous system (1 ~ 4294967295)
Redistribute local routes	<ul style="list-style-type: none"> ● Off: Not redistribute local routes from the device's own routing table. ● On : Redistribute local routes from the device's own routing table.
Redistribute connected routes	<ul style="list-style-type: none"> ● Off: Not redistribute connected routes to networks which are directly connected to the device. ● On: Redistribute connected routes to networks which are directly connected to the device.
Redistribute RIP routes	<ul style="list-style-type: none"> ● Off: Not redistribute RIP routes learned via the RIP routing protocol. ● On: Redistribute RIP routes learned via the RIP routing protocol.
Redistribute OSPF routes	<ul style="list-style-type: none"> ● Off: Not redistribute OSPF routes learned via the OSPF routing protocol. ● On: Redistribute OSPF routes learned via the OSPF routing protocol.

(2) Neighbor Configuration

The neighbors sub configuration is used to configure all the BGP routers to peer with and the maximum neighbors is 16.

BGP

General **Neighbors** Networks

Summary

#	Mode	IP Address	AS Number	Multihop	Edit	Delete
1	on	192.168.1.105	1	on		

Add BGP Neighbor **Add/Edit**

Mode Off On

IP Address IP address of the peer router

AS Number Autonomous system number of the peer router

Multihop Off On Allow multiple hops between this router and the peer router

IP Routing > BGP > Neighbor	
Item	Description
Neighbor	
Mode	Select from Off or On to enable the neighbor setting
IP Address	Set IP address of the peer router
AS Number	Autonomous system number of the peer router
Multihop	Allow multiple hops between this router and the peer router

(3) Networks Configuration

The networks sub configuration allows to add IP network prefixes that shall be distributed via BGP in addition to the networks that are redistributed from other sources as defined on the general sub configuration and the maximum neighbors is 16.

BGP

General Neighbors **Networks**

#	Mode	Prefix	Prefix Length	Edit	Delete
1	on	4.4.4.0	24		

Summary

Add BGP Network **Add/Edit**

Mode Off On

Prefix Prefix of the network

Prefix Length Length of the prefix

IP Routing > BGP > Networks	
Item	Description
Networks	
Mode	Select from Off or On to enable the network
Prefix	Set Prefix of the network
Prefix Length	Set Length of the prefix


10 Configuration > Service

This section allows you to configure OpenVPN, IPsec, Port Forwarding, Dynamic DNS, DMZ, SNMP, IP Filter, MAC Filter, URL Filter, VRRP, MQTT, UPnP, SMTP, NAT, IP Alias and GRE.













10.1 Service > Configuration OpenVPN

10.1.1 Edit OpenVPN Connection

- (1) This section allows you to configure the OpenVPN parameters. The default mode is Disable. Click  button to edit OpenVPN Connection.

The screenshot shows the "Open VPN" configuration page. At the top, there is a "Mode" section with radio buttons for "Disable" (selected) and "Enable". Below this is a table with 10 rows. Each row has columns for "#", "Mode", "VPN Mode", "Device", "Protocol", "Port", and "Edit". All "Mode" entries are "Disable", "VPN Mode" entries are "Client", "Device" entries are "TUN", "Protocol" entries are "UDP", and "Port" entries are "1701". Each "Edit" column contains a blue pencil icon. At the bottom right, there is an "Apply" button.

#	Mode	VPN Mode	Device	Protocol	Port	Edit
1	Disable	Client	TUN	UDP	1701	
2	Disable	Client	TUN	UDP	1701	
3	Disable	Client	TUN	UDP	1701	
4	Disable	Client	TUN	UDP	1701	
5	Disable	Client	TUN	UDP	1701	
6	Disable	Client	TUN	UDP	1701	
7	Disable	Client	TUN	UDP	1701	
8	Disable	Client	TUN	UDP	1701	
9	Disable	Client	TUN	UDP	1701	
10	Disable	Client	TUN	UDP	1701	

(2) From **Setting** tab, you can set up the connection of OpenVPN.

The screenshot displays the configuration page for an OpenVPN connection. On the left is a navigation sidebar with categories: Status, System, WAN, LAN, Service, and Management. The 'Service' category is expanded, showing options like Open VPN, IPSec, Port Forwarding, Dynamic DNS, DMZ, SNMP, TR069, IP Filter, MAC Filter, URL Filter, VRRP, and MQTT. The 'Management' category is also visible at the bottom of the sidebar.

The main content area is titled 'Edit Open VPN Connection #1' and has two tabs: 'Setting' (active) and 'Log'. The 'Setting' tab contains the following configuration options:

- Mode:** Disable Enable
- VPN Mode:** Server Client Custom
- Status:** Idle
- TLS Mode:** Disable Enable
- Cipher:** BF-CBC
- IPv6 Mode:** Disable Enable
- Device:** TUN TAP
- Protocol:** UDP TCP
- Port:** 1701
- VPN Compression:** Disable Enable
- Authentication:** Certificate

Below these are sections for Client, NAT, and Client - Security:

- Client:**
 - Client Mode:** Roadwarrior
 - Server Address:** 0.0.0.0
 - Route Client Networks:** Off On
- NAT:**
 - 1:1 NAT:** Off On
- Client - Security:**
 - Root CA:**
 - Cert:**
 - Key:**
 - P12:**

At the bottom of the page, there are three buttons: 'Back', 'Refresh', and 'Apply'.

(3) From **Log** tab, the interface will be shown the status of connection to make you follow the situation whenever is successful or fail connection.

Edit Open VPN Connection #1

Setting
Log

Back
Refresh
Apply

Service > OpenVPN	
Item	Description
Mode	Turn on/off OpenVPN to select Disable or Enable.
VPN Mode	<ul style="list-style-type: none"> ● Server: Tick to enable OpenVPN server tunnel. ● Client: Tick to enable OpenVPN client tunnel. The default is Client. ● Custom: This option allows user to use the .ovpn configuration file to quickly set up VPN tunnel with third-party server or use the OpenVPN advanced options to be compatible with other servers.
Status	Display the status of OpenVPN.
TLS Mode	Select from Disable or Enable for data security. The default is Disable.
Cipher	The OpenVPN format of data transmission.
IPv6 Mode	Select from Disable or Enable. The default is Disable.
Device	Select from TUN or TAP. The default is TUN.
Protocol	Select from UDP or TCP Client which depends on the application. The default is UDP.
Port	Enter the listening port of remote side OpenVPN server.
VPN Compression	Select Disable or Enable to compress the data stream. The default is Disable.
Authentication	<ul style="list-style-type: none"> ● Select from two different kinds of authentication ways: Certificate or pkcs#12 Certificate. ● The pkcs#12 option is only available on the VPN client mode.

10.1.2 Set up OpenVPN Client

This section allows you configure the **OpenVPN client** route and authentication files. The files could be imported by clicking **Import** button and the file should be downloaded from OpenVPN server.

Client

Client Mode Roadwarrior

Server Address

Route Client Networks Off On

NAT

1:1 NAT Off On

Client - Security

Root CA

Cert

Key

P12

Service > OpenVPN > Client VPN Mode	
Item	Description
Client	
Client Mode	Only support the Roadwarrior mode.
Server Address	Fill in WAN IP of OpenVPN server.
Route Client Networks	Select from Off or On. This setting needs to match the server side. When enabled, the 4G/LTE Router will auto apply the properly routing rules.
NAT	
1:1 NAT	<ul style="list-style-type: none"> • Tick to enable NAT Traversal for OpenVPN. This item must be enabled when the router under NAT environment. • Select from Off or On. • When two routers' LAN Subnet are same and create OpenVPN tunnels, this function should be turned on.
Client-Security	
Root CA	The Certificate Authority file of OpenVPN server could be downloaded from OpenVPN server.
Cert	The certification file is for OpenVPN client, which could be downloaded from OpenVPN server.
Key	The private key file is for OpenVPN client, which could be downloaded from OpenVPN server.
P12	The PKCS#12 file is for OpenVPN client, which could be downloaded from OpenVPN server.

10.1.3 Set up OpenVPN Server

This section allows you to configure the **server status of VPN Mode**.

Note: When selecting the **On** option of Route Client Networks, the OpenVPN server will route the client traffic or not. You should fill in the client IP and netmask when this option is enabled.

Server

Client Mode Roadwarrior

VPN Network

VPN Netmask

Roadwarrior

Route Client Networks Off On

NAT

1:1 NAT Off On

Server - Server Security

Root CA

Cert, Key

Server - User Security



User 1	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 2	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 3	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 4	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 5	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 6	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 7	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 8	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>

Service > OpenVPN > Server VPN Mode	
Item	Description
Server	
Client Mode	Only support the Roadwarrior mode.
VPN Network	The network ID for OpenVPN virtual network.
VPN Netmask	The netmask for OpenVPN virtual network.
Roadwarrior: Route Client Networks	Select from Off or On. The OpenVPN server will route the client traffic or not. User should fill in the client IP and netmask when this option is enabled.
NAT	
1:1 NAT	<ul style="list-style-type: none"> • Tick to enable NAT Traversal for OpenVPN. This item must be enabled when router under NAT environment. • Select from Off or On. The default is Off. • When two routers' LAN Subnet are same and create OpenVPN tunnels, this function is turned on.
Server- Server Security	
Root CA	Create Root CA key.
Cert, Key and DH	Create Cert, Key and DH key.
Server- User Security	
User 1 - User 8	According to your requirement, you can create different kinds of user security key from User 1 to User 8.

10.1.4 Set up OpenVPN Custom

For **Custom of VPN Mode**, this section helps you use the .ovpn configuration file to quickly set up VPN tunnel with third-party server or use the OpenVPN advance options to be compatible with other servers.

Note:

- When clicking the **Import** button, you can import third-party OpenVPN configuration that find out from Internet and save the document into your server or PC. After importing the file, the interface will show   button to click  for displaying the information and to click  for downloading the file.
- For third-party OpenVPN configuration, suggest from <http://www.vpngate.net/en/>

Edit Open VPN Connection #1

Setting

Log

Mode Disable Enable

VPN Mode Server Client Custom

Custom Config Import *.ovpn

Username

Password

Status Idle

Back

Refresh

Apply

Service > OpenVPN > Custom VPN Mode	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
VPN Mode	Select from custom mode.
Custom Config	Import OpenVPN configuration.
Username	Fill in the username if the imported file has already set up the username.
Password	Fill in the password if the imported file has already set up the password.
Status	Display the connection status of OpenVPN, such as IP address and the connected time.

10.2 Service > Configuration IPSec

This section allows you to set up IPSec Tunnel. The setting has two tags, General setting and Connections.

10.2.1 IPSec > General setting

For **General setting**, you can set up **IKE**, **Encryption** and **Authentication**. The General setting for the local and remote side should be the same when using Net-to-Net application.


The screenshot displays the configuration interface for an IPSec tunnel. On the left is a navigation sidebar with categories: Status, System, WAN, LAN, Service, and Management. The main panel is titled 'IPSec' and features a 'Mode' selector (Disable/Enable) and two tabs: 'General setting' (active) and 'Connections'. The configuration is organized into several sections:

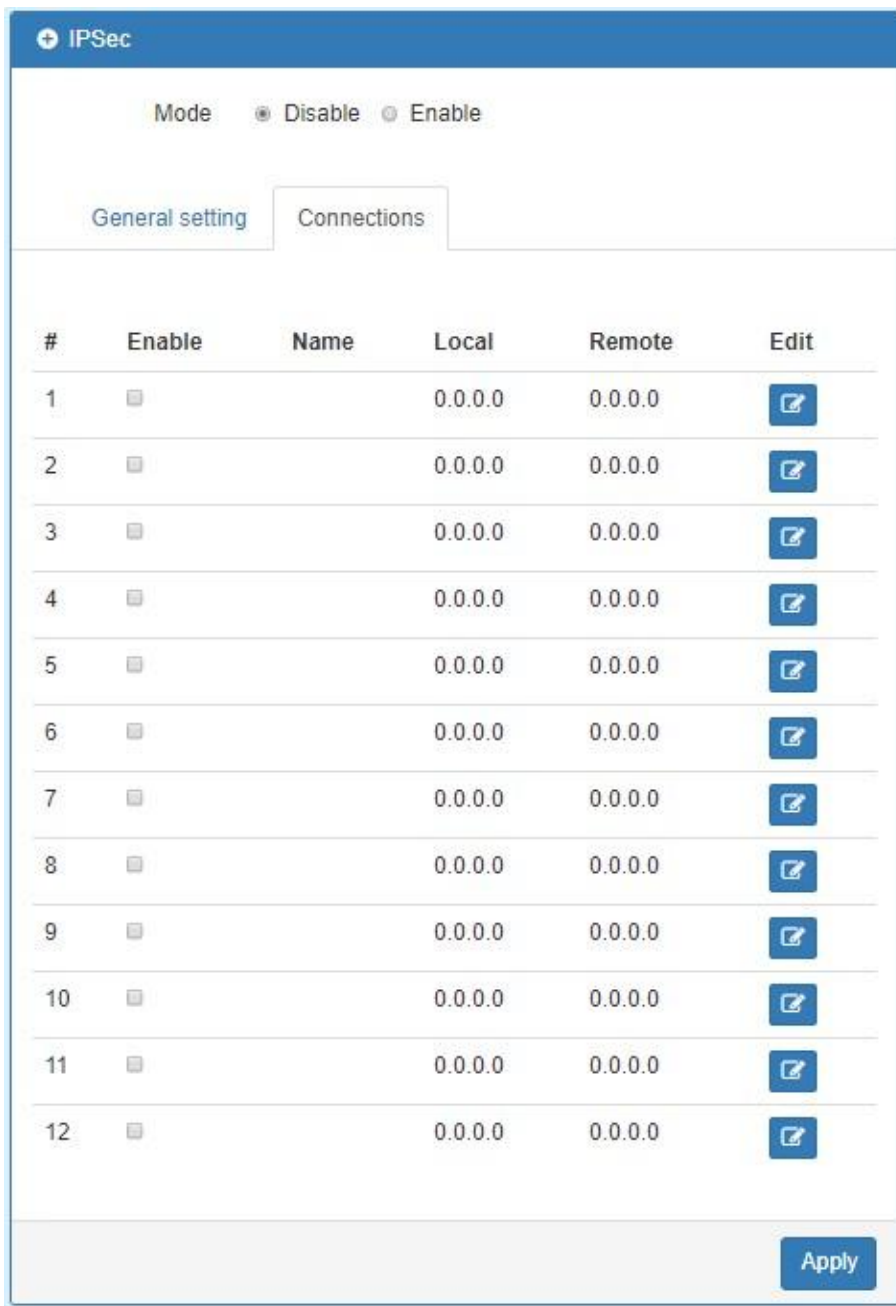
- IKE**: Protocol (IKEv1), Aggressive mode (Disable), Encryption (AES128), Hash (SHA1), and DH Group (5 (1536 bit)).
- Encryption**: Protocol (ESP), Encryption (AES128), Hash (SHA1), and DH Group (5 (1536 bit)).
- Authentication**: Auth Type (PSK) and an empty Auth Secret field.
- Advance**: DPD delay (30) and DPD timeout (150).

An 'Apply' button is located at the bottom right of the main panel. To the right of the main panel is a sidebar titled 'X.509 Certificates' with a search icon. It contains two sections: 'Create' with buttons for Root CA, Local, Remote, and Remote CA; and 'Import' with buttons for Local and Remote CA, each accompanied by 'Cert' and 'Key' sub-buttons.

Service > IPSec > General setting	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
IKE	
Protocol	Select from IKEv1 or IKEv2.
Aggressive mode	Select from Enable or Disable (default). (Note: The Aggressive mode is for IKEv2.)
Encryption	Select from AES128 (default), AES192, AES256 or 3DES.
Hash	Select from MD5, SHA1 (default) or SHA256.
DH Group	Select from 1(768 bit), 2(1024 bit), 5(1536 bit) (default), 14(2048 bit), 15(3072 bit), 16(4096 bit), 17(6144 bit) or 18(8192 bit).
Encryption	
Protocol	Select from ESP.
Encryption	Select from AES128 (default), AES192, AES256, 3DES or DES.
Hash	Select from MD5, SHA1 (default) or SHA256.
DH Group	Select from off, 1(768 bit), 2(1024 bit), 5(1536 bit) (default), 14(2048 bit), 15(3072 bit), 16(4096 bit), 17(6144 bit) or 18(8192 bit).
Authentication	
Auth Type	Select from PSK (default) or RSA. (Note: The EAP-TLS is for IKEv2.)
Auth Scret	The password is for PSK authentication type.
Advance	
DPD delay (Deed Peer Detection)	Define the period time interval to detect dead peers. The default is 30 seconds.
DPD timeout (Deed Peer Detection)	Define the timeout interval, after which all connections to a peer are deleted in case of inactivity. The default is 150 seconds.

10.2.2 IPSec > Connections













For **Connections** tab, the web UI provides the overview for each connection. Click  button to edit IPSec connection and set up the local and remote side.



IPSec

Mode Disable Enable

General setting **Connections**

#	Enable	Name	Local	Remote	Edit
1	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
2	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
3	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
4	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
5	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
6	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
7	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
8	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
9	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
10	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
11	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
12	<input type="checkbox"/>		0.0.0.0	0.0.0.0	

Apply

Edit IPSec Connection #1

Mode Disable Enable

Name

Status Idle

Local

Host

Subnet

ID

Remote

Host

Subnet

ID

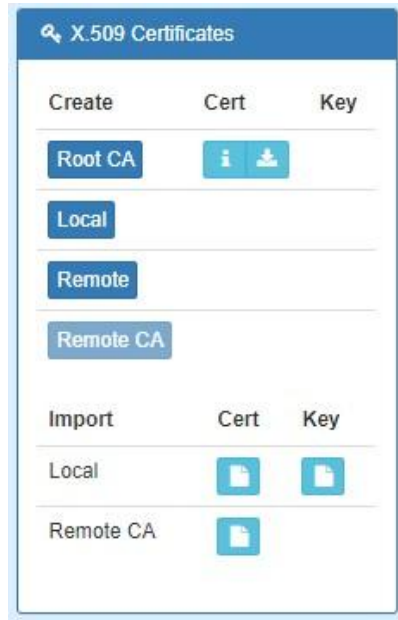
[Save](#)

Service > IPSec > Connections	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Name	Fill in the name of IPSec Tunnel.
Status	Display the connection status of IPSec.
Local	
Host	Fill in the WAN IP of 4G/LTE Router.
Subnet	Fill in the subnet for the LAN of 4G/LTE Router.
ID	The connection ID of IPSec local side.
Remote	
Host	Fill in the granted remote IP. If no limitation, keep blank.
Subnet	Fill in the granted remote subnet. If no limitation, keep blank.
ID	The connection ID of IPSec Remote side.

10.2.3 IPSec > The setting of X.509 Certificates

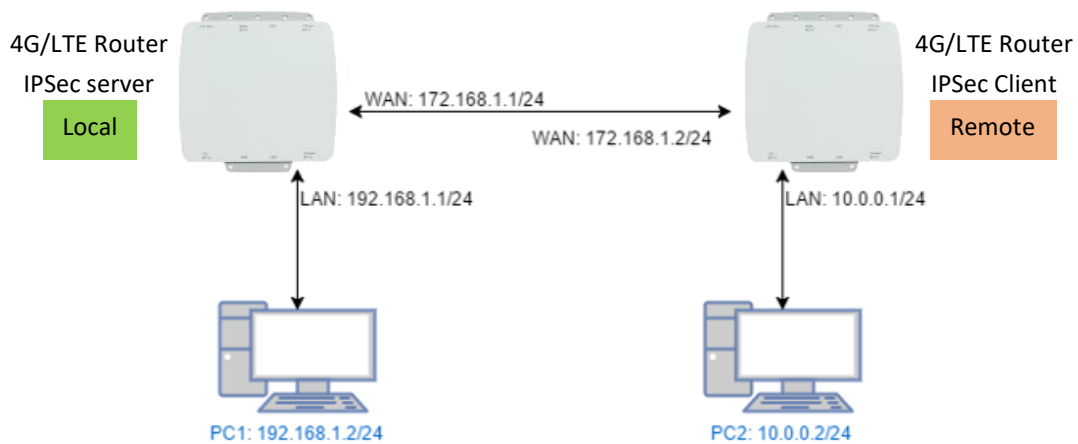
The interface shows the setting items of X.509 Certificates.

- You need to create the IPSec Security Keys by clicking Create button, including Root CA, Local, Remote and Remote CA. E.g. To create Root CA file, click the Root CA button.
- For the IPSec connection, the client should set up properly Root CA, Local, Remote and Remote CA key and cert files. The files could be downloaded by clicking ↓ Download button after the file generated.
- You can import the files of local and remote CA from the server.



10.2.4 IPsec > Net-to-Net Configuration

In this case, the IPsec VPN tunnel uses the two LAN side subnet clouds and makes them communicate each other. There are two part settings for the 4G/LTE Router IPsec feature.



General setting

The first part is the general setting, it provides the IPsec basic setting and authentication configuration. The psk (Pre-shared key) is as an authentication option to simplify the progress. The general setting for the local and remote side should be used the same setting.

IPSec

Mode Disable Enable

General setting | Connections

IKE

Protocol: IKEv1

Aggressive mode: Disable

Encryption: AES128

Hash: SHA1

DH Group: 5 (1536 bit)

Encryption

Protocol: ESP

Encryption: AES128

Hash: SHA1

DH Group: 5 (1536 bit)

Authentication

Auth Type: PSK

Auth Secret:

Advance

DPD delay: 30

DPD timeout: 150

Apply

Connections Setting


The second part is the connection setting, you can configure the local and the remote side setting for each connection.

For the Net-to-Net scenario, you can configure the information of **Host**, **Subnet** and **ID** for the local and remote side. In this case, the #1 connection is edited from connections tab for setting up the Net-to-Net configuration.

IPSec

Mode Disable Enable

General setting | **Connections**

#	Enable	Name	Local	Remote	Edit
1	<input type="checkbox"/>		0.0.0.0	0.0.0.0	

- Local Side

First, fill up the local Host and Subnet fields by the network information of IPSec server.

And, use the network information of IPSec client to fill up the remote setting.

Then, specify the ID for the both sides.

In this case, the IDs for the local and remote side are named as @local and @remote respectively.

Note: The ID should be started with @ symbol. The above settings will make the traffic between 192.168.1.0/24 and 10.0.0.0/24. They can be forwarded by IPSec tunnel.

Edit IPSec Connection #1

Mode Disable Enable

Name

Status Established

Local

Host

Subnet

ID

Remote

Host

Subnet

ID

- Remote Side

The setting for remote side is similar to Local Side. Just swap the local settings with the remote setting.

Edit IPSec Connection #1

Mode Disable Enable

Name

Status Established

Local

Host

Subnet

ID

Remote

Host

Subnet

ID

The mapping is as below:

- 1. Root CA (Local side) -> Import Remote CA (Remote side)
- 2. Remote Cert (Local side) -> Import Local Cert (Remote side)
- 3. Remote Key (Local side) -> Import Local Key (Remote side)

For Connection setting, the mapping of connection IDs like the following table.

Certificate	IPSec local side	IPSec remote side
Local	@local.ipsec	@remote.ipsec
Remote	@remote.ipsec	@local.ipsec

Local Side

Edit IPSec Connection #1

Mode Disable Enable

Name

Status Connecting

Local

Host

Subnet

ID

Remote

Host

Subnet

ID

Remote Side

Edit IPSec Connection #1

Mode Disable Enable

Name

Status Connecting

Local

Host

Subnet

ID


Remote

















Host

Subnet

ID

10.3 Service > Configuration Port Forwarding

This section allows you to set up Port Forwarding and click  edit button to configure.

Port Forwarding				
Mode <input checked="" type="radio"/> Disable <input type="radio"/> Enable				
#	Mode	Description	Protocol	Edit
1	Disable	ssh	TCP	
2	Disable		TCP	
3	Disable		TCP	
4	Disable		TCP	
5	Disable		TCP	
6	Disable		TCP	
7	Disable		TCP	
8	Disable		TCP	
9	Disable		TCP	
10	Disable		TCP	
11	Disable		TCP	
12	Disable		TCP	
13	Disable		TCP	
14	Disable		TCP	
15	Disable		TCP	
16	Disable		TCP	

Edit Port Forwarding Entry #1

Mode Disable Enable

Description

Protocol TCP UDP

Source Port Begin

Source Port End

Destination IP

Destination Port Begin

Destination Port End

Service > Port Forwarding	
Item	Description
Mode	Turn on/off Port Forwarding to select Disable or Enable. The default is Disable.
Description	Describe the name of Port Forwarding.
Protocol	Select from UDP or TCP Client which depends on the application.
Source Port Begin	Fill in the beginning of source port.
Source Port End	Fill in the end of source port.
Destination IP	Fill in the current private destination IP.
Destination Port Begin	Fill in the beginning of private destination port.
Destination Port End	Fill in the end of private destination port.

10.4 Service > Dynamic DNS

This section allows you to set up Dynamic DNS.

+ Dynamic DNS

Mode Disable Enable

Service Provider

Host Name

Token ID

Update Period Time (Sec)

+ Dynamic DNS

Mode Disable Enable

Service Provider

Host Name

Token ID

Update Period Time (Sec)

Service > Dynamic DNS	
Item	Description
Mode	Turn on/off this function to select Disable or Enable. The default is Disable.
Service Provider	Select the Service Provider of Dynamic DNS.
Host Name	Fill in your registered Host Name from Service Provider.
Token ID	Fill in your Token ID from Service Provider.
Host Secret ID	Fill in your Secret ID from Service Provider.
Username	Fill in your registered username from Service Provider.
Password	Fill in your registered password from Service Provider.
Update Period Time (Sec)	Fill in "0" to mean 30 days.

Note: There are five options of Service Provider as below to explain the information.

Service Provider	dynv6.com
Host Name	Register hostname, e.g. tester.dynv6.net
Token ID	The token ID, e.g. v_ABjMMQxeAnWv5UwtuVn1QBriynzq

Service Provider	www.nsupdate.info
Host Name	Register hostname, e.g. tester.nsupdate.info
Host Secret ID	The Host Secret ID, e.g. e2AMDsLmVF

Service Provider	www.duckdns.org
Host Name	Register hostname, e.g. tester.duckdns.org
Token ID	The token ID, e.g.12345678-de49-4e97-a33c-98b159aead2b

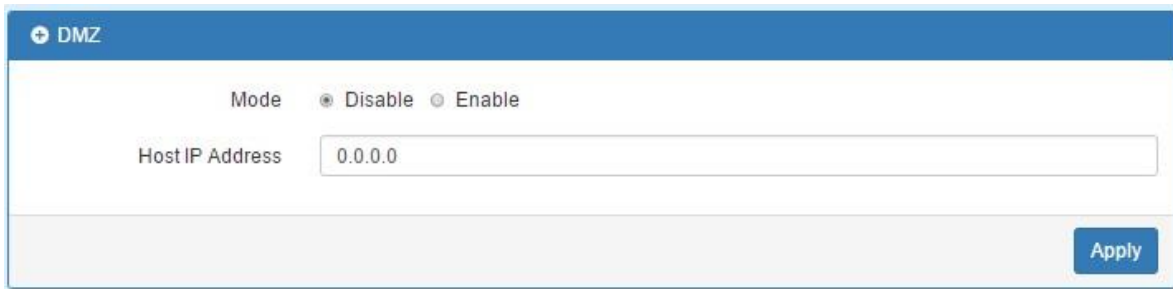
Service Provider	no-ip.com
Host Name	Register hostname, e.g. tester.hopto.org
Username	Register username.
Password	Register password.

Service provider	freedns.afraid.org
Host Name	Register hostname, e.g. tester.mooo.com
Username	Register username.
Password	Register password.

Service provider	dyndns.org
Host Name	Register hostname, e.g. tester.dyns.com
Username	Register username.
Password	Register password.

10.5 Service > DMZ

This section allows you to set the DMZ configuration.

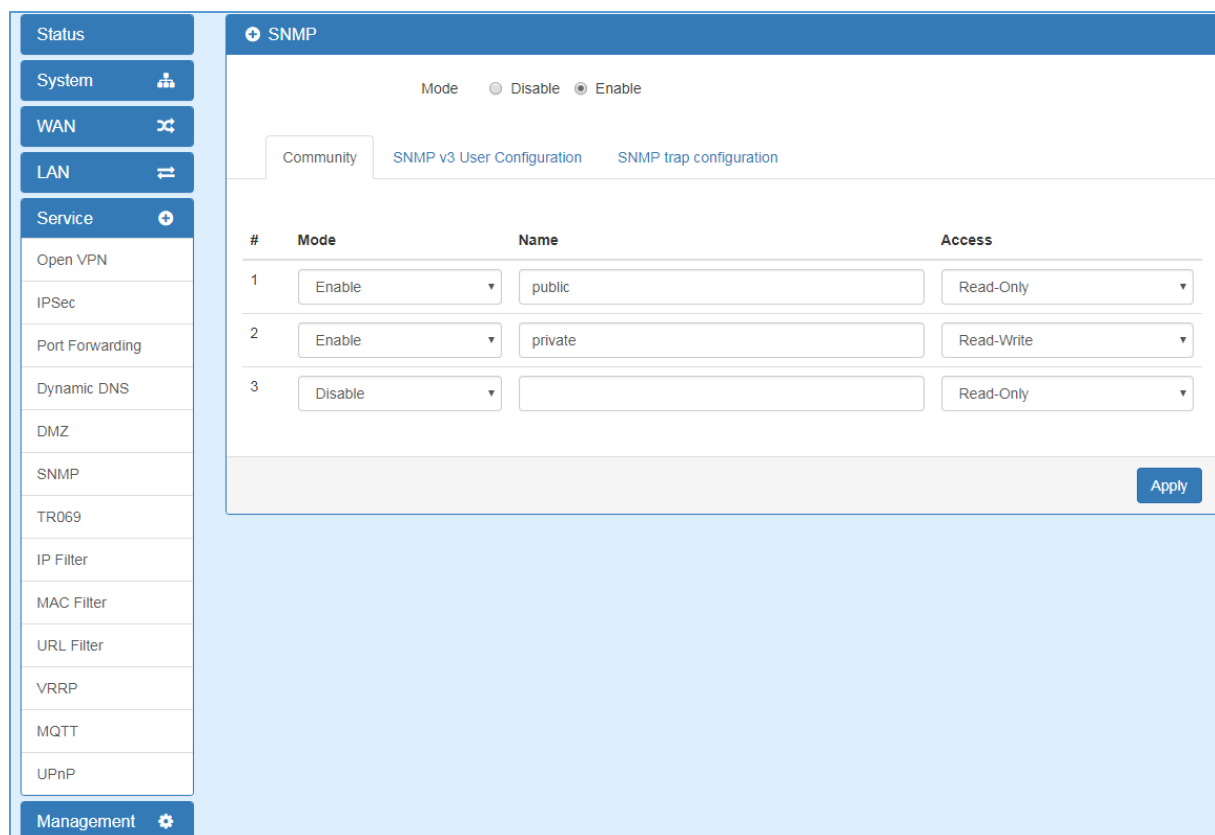


Service > DMZ	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Host IP Address	Fill in your Host IP Address.

10.6 Service > SNMP

10.6.1 SNMP configuration

This section allows you to set the SNMP configuration.



#	Mode	Name	Access
1	Enable	public	Read-Only
2	Enable	private	Read-Write
3	Disable		Read-Only

Service > SNMP > Community	
Item	Description
Mode	Select from Disable or Enable to configure SNMP.
Community	Configure community setting with three options, including # 1, # 2 and #3.
Mode	Select from Disable or Enable.
Name	Name each community.
Access	Select from Read-Only or Read-Write.

10.6.2 SNMP v3 User configuration

For SNMP version 3, you need to register authentication and allow a receiver that confirm the packet was not modified in transit. There are three options to set up SNMP v3 configuration.

Service > SNMP > SNMP v3 User configuration	
Item	Description
Mode	Select from Disable or Enable to configure SNMP. The default is Disable.
Name	Fill in your name.
Auth Mode	Select from Authentication or Privacy.
Authentication Password	Fill in your authentication password.
Authentication Protocol	Select from MD5 or SHA.
Privacy Password	Fill in your privacy password.
Privacy Protocol	Select from DES or AES.
Access	Select from Read-Only or Read-Write.

10.6.3 SNMP trap configuration

This section allows you to set up the SNMP trap configuration when you select the **SNMP trap** function from Alarm output of system for your router. With SNMP trap setting, you can know the status of remote device.

Service > SNMP > SNMP trap configuration	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Community Name	Fill in your community name.
Destination	The destination (domain name/IP) of remote SNMP trap server.

10.7 Service > TR069

This section allows you to set up TR069 client configuration. You can get information how to install TR069 Server (GenieACS Installation) from the application configuration chapter.

TR069

Mode Disable Enable

ACS URL

ACS Username

ACS Password

Periodic Inform Disable Enable

Periodic Inform Interval(Sec)


Connection Request Username

Connection Request Password

[Apply](#)

















Service > TR069	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
ACS URL	Fill in the URL address of ACS (Auto-Configuration Server).
ACS Username	Fill in the ACS username to authenticate the CPE (this router) when connecting to the ACS.
ACS Password	Fill in the ACS password to authenticate the CPE (this router) when connecting to the ACS.
Periodic Inform	Select from Disable or Enable. The default is Disable. The CPE reports the status to the ACS when enabling a period of time set.
Periodic Inform Interval(Sec)	Fill in the periodic time. The CPE reports to ACS the status according to your duration in seconds of the interval set.
Connection Request Username	Fill in the connection request username to authenticate the ACS if the ACS attempts to communicate with the CPE connecting.
Connection Request Password	Fill in the connection request password to authenticate the ACS if the ACS attempts to communicate with the CPE connecting.

10.8 Service > IP Filter

This section allows you to configure IP Filter. After clicking  button, you can edit your IP protocol, source/port and destination/port.

IP Filter

Mode Disable Enable

#	Mode	Protocol	Source / Port	Destination / Port	Edit
1	Disable	All	0.0.0.0 --	0.0.0.0 --	
2	Disable	All	0.0.0.0 --	0.0.0.0 --	
3	Disable	All	0.0.0.0 --	0.0.0.0 --	
4	Disable	All	0.0.0.0 --	0.0.0.0 --	
5	Disable	All	0.0.0.0 --	0.0.0.0 --	
6	Disable	All	0.0.0.0 --	0.0.0.0 --	
7	Disable	All	0.0.0.0 --	0.0.0.0 --	
8	Disable	All	0.0.0.0 --	0.0.0.0 --	
9	Disable	All	0.0.0.0 --	0.0.0.0 --	
10	Disable	All	0.0.0.0 --	0.0.0.0 --	
11	Disable	All	0.0.0.0 --	0.0.0.0 --	
12	Disable	All	0.0.0.0 --	0.0.0.0 --	
13	Disable	All	0.0.0.0 --	0.0.0.0 --	
14	Disable	All	0.0.0.0 --	0.0.0.0 --	
15	Disable	All	0.0.0.0 --	0.0.0.0 --	
16	Disable	All	0.0.0.0 --	0.0.0.0 --	

Apply

(1) The default is Disable Mode as the following interface.

The screenshot shows a configuration window titled "Edit IP Filter Black List Entry #1". It contains several fields:

- Mode:** Radio buttons for "Disable" (selected) and "Enable".
- Protocol:** Radio buttons for "All" (selected), "ICMP", "TCP", and "UDP".
- Source IP:** Text input field containing "0.0.0.0".
- Source Port:** Text input field containing "0".
- Destination IP:** Text input field containing "0.0.0.0".
- Destination Port:** Text input field containing "0".

 A blue "Save" button is located at the bottom right of the form.

Service > IP Filter	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Protocol	Select from All, ICMP, TCP or UDP.
Source IP	Fill in your source IP address.
Source Port	Fill in your source port.
Destination IP	Fill in your destination IP address.
Destination Port	Fill in your destination port.

(2) When selecting Enable Mode, the protocol is TCP. The source IP has IPv4 and IPv6 setting formats.

(3) For Source IP, there are three types to input your source IP that depends on your requirement, including single IP, IP with Mask or giving a range of IP. The following table provides some examples.


Service > Edit IP Filter > Source IP			
IP Format	Single IP	IP with Mask	Ranged IP
IPv4	192.168.0.123	192.168.1.0/24 192.168.1.0/255.255.255.	192.168.1.1-192.168.1.123
IPv6	2607:f0d0:1002:51::4	2607:f0d0:1002:51::0/64	2607:f0d0:1002:51::4- 2607:f0d0:1002:51::aaaa

Note: Setting up a range of IP, please use – hyphen symbol to mark your ranged IP.

(4) For Source Port, there are two types to input your source port that depends on your requirement, including single port (e.g.1234) or giving a range of ports (e.g.1234:5678).

















Note: Setting up a range of source ports, please use : colon symbol to mark your ranged ports.

10.9 Service > MAC Filter

This section allows you to set up MAC Filter. After clicking  button, you can edit your MAC address.

+ MAC Filter

Mode Disable Enable

#	Mode	MAC Address	Edit
1	Disable		
2	Disable		
3	Disable		
4	Disable		
5	Disable		
6	Disable		
7	Disable		
8	Disable		
9	Disable		
10	Disable		
11	Disable		
12	Disable		
13	Disable		
14	Disable		
15	Disable		
16	Disable		

Edit MAC Filter Black List Entry #1


Mode Disable Enable

















MAC Address

Service > MAC Filter	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
MAC Address	Fill in your MAC address.

Note: Setting up MAC address, please use : colon symbol (e.g. xx : xx : xx: xx) or – hyphen symbol to mark (e.g. xx- xx-xx-xx).

10.10 Service > URL Filter

This section allows you to set up URL Filter. After clicking  button, you can edit the type of filter and information.

URL Filter				
Mode <input checked="" type="radio"/> Disable <input type="radio"/> Enable				
#	Mode	Filter	Key/Full	Edit
1	Disable	Key		
2	Disable	Key		
3	Disable	Key		
4	Disable	Key		
5	Disable	Key		
6	Disable	Key		
7	Disable	Key		
8	Disable	Key		
9	Disable	Key		
10	Disable	Key		
11	Disable	Key		
12	Disable	Key		
13	Disable	Key		
14	Disable	Key		
15	Disable	Key		
16	Disable	Key		

Apply

Edit URL Filter Black List Entry #1

Mode Disable Enable

Filter Key Full Hint: Please NOT include 'https://' inside the URL

Key/Full

Save

Note: Please not include “https://” for the URL address in the **Full** Filter.

Mode Disable Enable

Filter Key Full

Key/Full

Service > URL Filter	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Filter	Select from Key or Full. The default is Key.
Key/Full	Fill in your Key/Full information.

10.11 Service > VRRP

This section allows you to configure VRRP.

+ VRRP

Mode Disable Enable

Group ID

Priority

Virtual IP

Service > VRRP	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Group ID	Specify which VRRP group of this router belong to (1-255). The default is 1.
Priority	Enter the priority value from 1 to 254. The larger value has higher priority. The default is 100.
Virtual IP	<ul style="list-style-type: none"> ● Each router in the same VRRP group must have the same virtual IP address. The default is 0.0.0.0. ● This virtual IP address must belong to the same address range as the real IP address of the interface.

10.12 Service > MQTT

This section makes you configure MQTT which allows the MQTT client to send the message within specific topic or channel. By default, the router does not allow anonymous to read/write the MQTT topic or channel. Thus, you need to create the account with username and password for MQTT client in the web UI.

+ MQTT

Mode Disable Enable

Port

Manage Users

Name	Delete
Username <input style="width: 150px;" type="text"/>	
Password <input style="width: 150px;" type="text"/>	
<input type="button" value="Add"/>	

ACLs

User	Topic	Read	Write	Delete
User <input style="width: 150px;" type="text"/>	Topic <input style="width: 150px;" type="text"/>	<input type="checkbox"/> Read	<input type="checkbox"/> Write	
<input type="button" value="Add"/>				

Service > MQTT	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Port	Fill in the port number of MQTT application.
Manage Users	Create the users and show all users' names. Allow each user to delete their name.
Username	Fill in the username of manage user.
Password	Fill in the password of manage user.
ACLs	Allow to specify what topic should be limited.
User	Select the users and identify their authority to read or write the MQTT topic/channel.
Topic	Name the topic of MQTT message.

Take for example, the interface is shown as below.

The Manage Users section will show all users that you create. Moreover, each user can use the delete button to delete it. For the ACL control, user can specify what topic should be limited. In this case, we set up the publisher **pub1** to write the critical topic. Additionally, we also allow the subscribers **sub1** and **sub3** to read the critical topic. Thus, only the sub1 and sub3 can receive it when **pub1** sending the message.

MQTT

Mode Disable Enable

Port

Manage Users

Username	Password	Delete
<input type="text" value="Sub1"/>	<input type="password" value="...."/>	<input checked="" type="button" value="x"/>
<input type="text" value="Sub2"/>	<input type="password" value="...."/>	<input checked="" type="button" value="x"/>
<input type="text" value="Sub3"/>	<input type="password" value="...."/>	<input checked="" type="button" value="x"/>
<input type="text" value="Pub1"/>	<input type="password" value="...."/>	<input checked="" type="button" value="x"/>
<input type="text" value="Pub2"/>	<input type="password" value="...."/>	<input checked="" type="button" value="x"/>

Username

Password

ACLs

User	Topic	Read	Write	Delete
<input type="text" value="Sub1"/>	<input type="text" value="Critical"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="button" value="x"/>
<input type="text" value="Sub3"/>	<input type="text" value="Critical"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="button" value="x"/>
<input type="text" value="Pub2"/>	<input type="text" value="Critical"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="button" value="x"/>

User

Topic

Read

Write

10.13 Service > UPnP

This section allows you to set up UPnP configuration to select the mode from Disable or Enable. The default UPnP is enabled for the 4G/LTE Router.



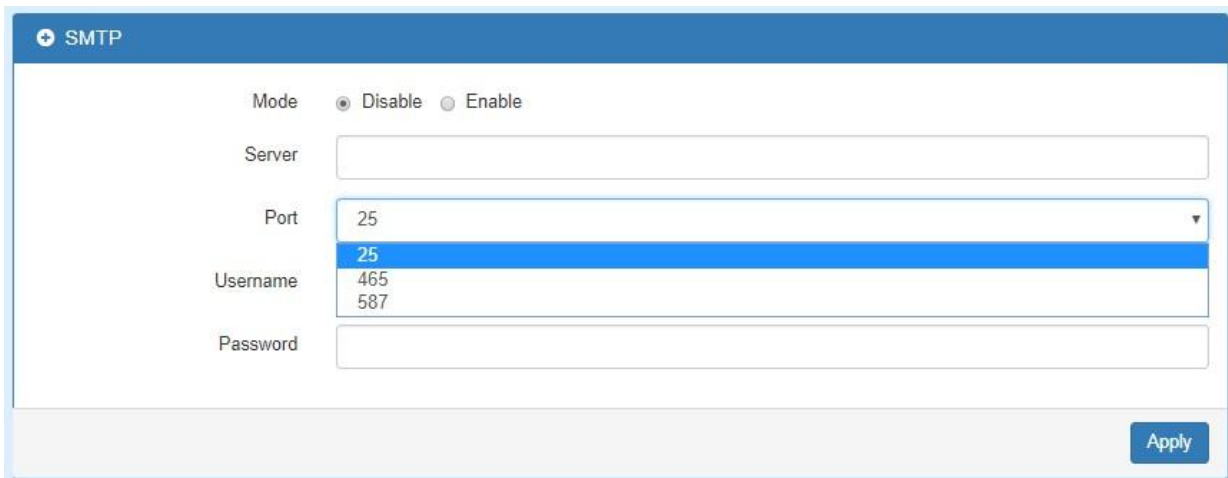
Note:

UPnP™ (Universal Plug and Play) is a set of protocols that allows a PC to automatically discover other UPnP devices (anything from an Internet gateway device to a light switch), retrieve an XML description of the device and its services, control the device, and subscribe to real-time event notification.

PCs using UPnP can retrieve the 4G/LTE Router's WAN IP address, and automatically create NAT port maps. This means that applications that support UPnP, and are used with UPnP enabled 4G/LTE Router, will not need application layer gateway support on the 4G/LTE Router to work through NAT.

10.14 Service > SMTP

This section provides you to send your email for the server. For instance, the email will be sent to notify when the Alarm has a notification by the server.



Service > SMTP	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Server	The email will be sent through the server.
Port	There are three ports for SMTP communication between mail servers. <ul style="list-style-type: none">● Port 25 : Use TCP port 25 without encryption.● Port 465 : SMTP connections secured by SSL.● Port 587 : SMTP connections secured by TLS.
Username/Password	Fill in your username and password as the same your server.

10.15 Service > NAT

This section allows you to set NAT configuration.

When NAT is on, the router will replace the source private IP address by its Internet public address for outgoing packets, and replace the destination Internet public address by private IP address for incoming packets.

When NAT is off, the router will send the source LAN private IP address for outgoing packets and allow to receive the destination LAN private IP address for incoming packets.



NAT

Mode Disable Enable

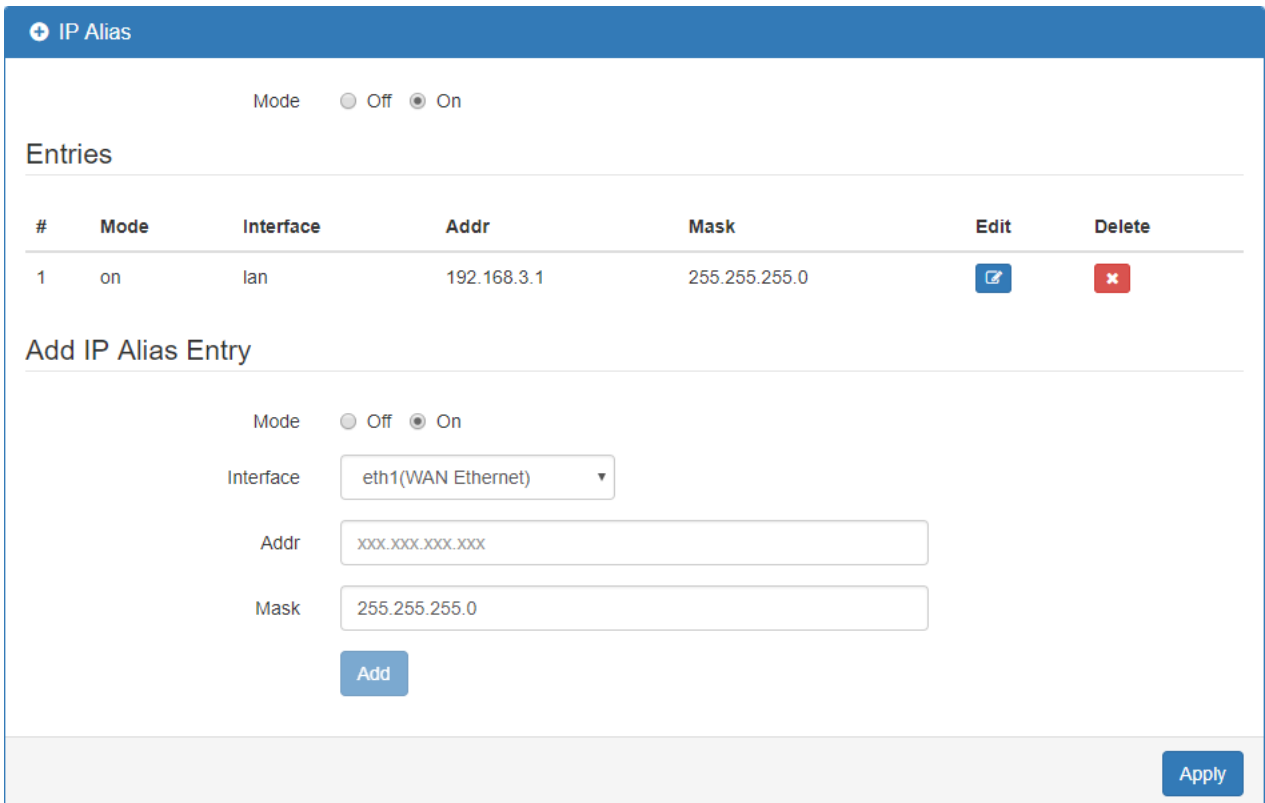
Apply

10.16 Service > IP Alias

This section allows you to set **IP Alias** configuration.

IP Alias is associating more than one IP address to a network interface. With IP Alias, one node on a network can have multiple connections to a network, each serving a different purpose.



IP Alias can be used to provide multiple network addresses on a single physical interface.



IP Alias

Mode Off On

Entries

#	Mode	Interface	Addr	Mask	Edit	Delete
1	on	lan	192.168.3.1	255.255.255.0		

Add IP Alias Entry

Mode Off On

Interface

Addr

Mask

Add

Apply

Service > IP Alias	
Item	Description
Mode	Select from Off or On to enable the IP Alias.
Entries	The setting can be edited or deleted the existed entries.
Add/Edit IP Alias Entry	<ul style="list-style-type: none"> ● Mode: select from Off or On to use or not use this entry. ● Interface: the interface you want to provide the additional address. ● Addr: the IP address. ● Mask: the network mask.

10.17 Service > GRE

This section allows you to set GRE configuration. The default mode is off.

Generic Routing Encapsulation (GRE) is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

The screenshot shows the GRE configuration page with the title '+ GRE'. Under the 'Mode' section, the 'Off' radio button is selected, and the 'On' radio button is unselected. An 'Apply' button is visible in the bottom right corner.

The GRE Mode is on.

The screenshot shows the GRE configuration page with the title '+ GRE'. Under the 'Mode' section, the 'On' radio button is selected, and the 'Off' radio button is unselected. Below the mode section, there are four input fields: 'Local Address' (192.168.1.4), 'Remote Address' (192.168.1.5), 'Tunnel Device Address' (10.1.1.4), and 'Tunnel Device Address Prefix' (8). An 'Apply' button is visible in the bottom right corner.

Service > IP Alias	
Item	Description
Mode	Select from Off or On to enable GRE.
Local Address	Set local address of the GRE tunnel.
Remote Address	Set remote address of the GRE tunnel.
Tunnel Device Address	Set IP address of this GRE tunnel device.
Tunnel Device Address Prefix	Set Prefix of the Tunnel Device Address.

11 Management

This section provides you to manage the router, set up your administration and know about the status of current software and firmware. Also, you can back up and restore the configuration.



11.1 Identification

This section allows you to confirm the profile of router, current software, firmware version and system uptime.

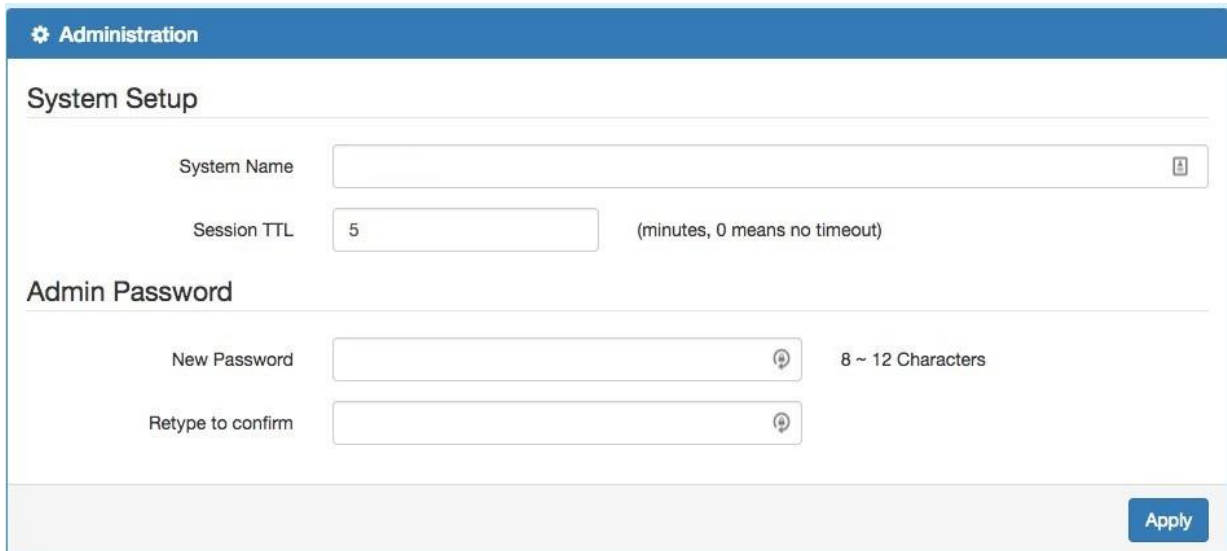


Attr.	Value
Host Name	OLTRG-100
MAC Address	00:1B:5C:11:22:33
Software Version	V 1.64
Software MCSV	012C000015029A6F
Hardware MCSV	012C000000000000
Modem Firmware Version	EC25EFAR02A04M4G
System Uptime	02:34

Management > Identification	
Item	Description
Host Name	Show the host name of 4G/LTE Router.
MAC Address	Show the MAC address.
Software Version	Show the current software version.
Software MCSV	Show the current software MCSV.
Hardware MCSV	Show the current hardware MCSV.
Modem Firmware Version	Show the current firmware version.
System Uptime	Show the current system uptime.

11.2 Administration

This section allows you to set up the name of system and change your new password. For the Session TTL, you can set up what duration of time will be logout. If you don't need to have this timeout limitation, you can fill in "0"(Zero).



The screenshot shows the 'Administration' section with a 'System Setup' sub-section. It contains two input fields: 'System Name' and 'Session TTL' (set to 5 minutes). Below this is the 'Admin Password' section with 'New Password' and 'Retype to confirm' fields. A blue 'Apply' button is at the bottom right.

11.3 Firmware

This section provides you to upgrade the firmware of router.

- (1) Click **Select the firmware to upgrade** button to choose your current firmware version in your PC.
- (2) Select **Upgrade** button to update.
- (3) After upgrading successfully, the router will reboot automatically.

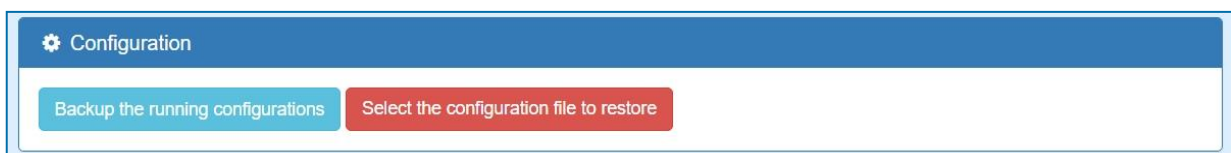


The screenshot shows the 'Firmware' section with a blue button labeled 'Select the firmware to upgrade(*.tar)' and a red 'Upgrade' button at the bottom right.

11.4 Configuration

This section supports you to export or import the configuration file.

- (1) Click **Backup the running configurations** button to export your current configurations.
- (2) Click **Select the configuration file to restore** button to import the configuration file.



The screenshot shows the 'Configuration' section with two buttons: a blue 'Backup the running configurations' button and a red 'Select the configuration file to restore' button.

11.5 Load Factory

This section supports you to load the factory default configuration and restart the device immediately. You can click the [Load Factory and Restart](#) button.



11.6 Restart

This section allows you to click [Restart](#) button and the router will restart immediately.

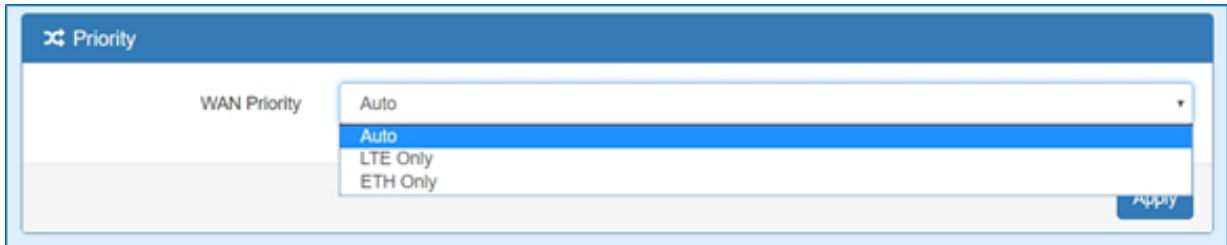


12 Configuration Applications

This section explains specific examples how to configure your applications.

12.1 WAN Priority

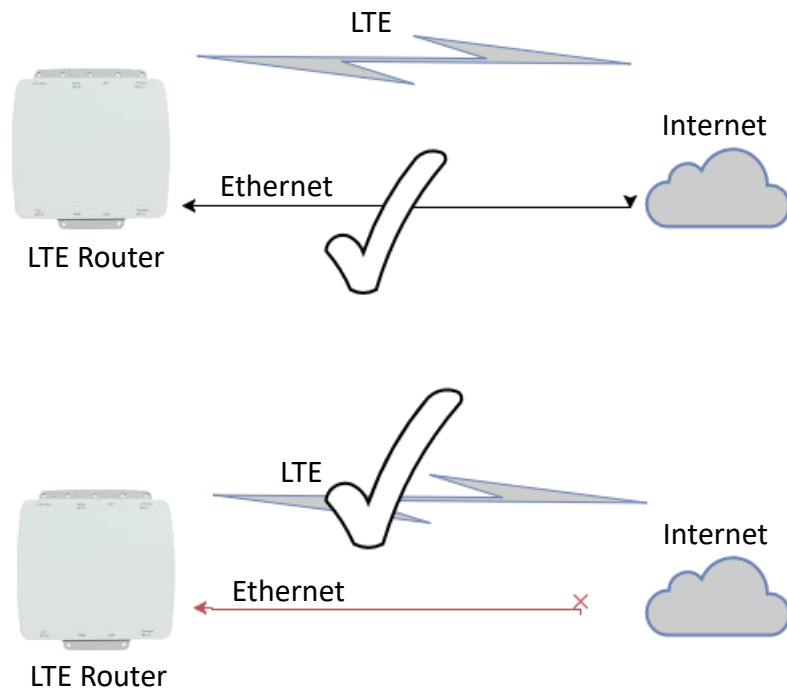
You can select from Auto, LTE Only or ETH Only.



(1) WAN Priority > Auto:

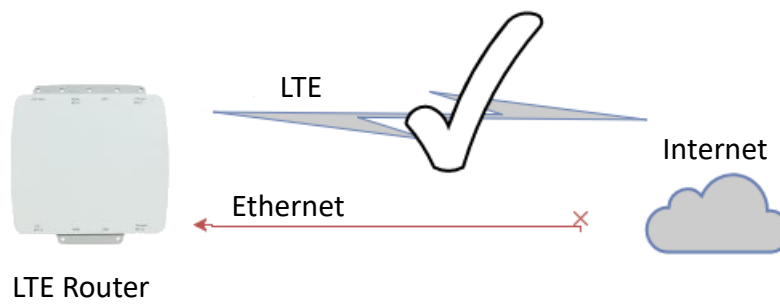
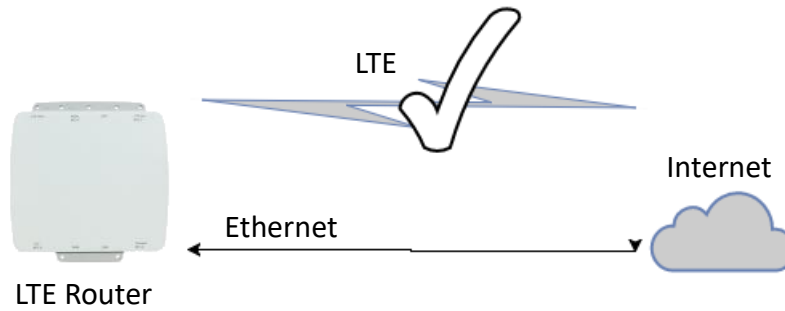
In case both Ethernet and LTE can access Internet, the router would route network packages through Ethernet. The reason is Ethernet that is low price and stable.

However, in case Ethernet is unplug or not able to access Internet (check by ping), the router would route network packages through LTE network.



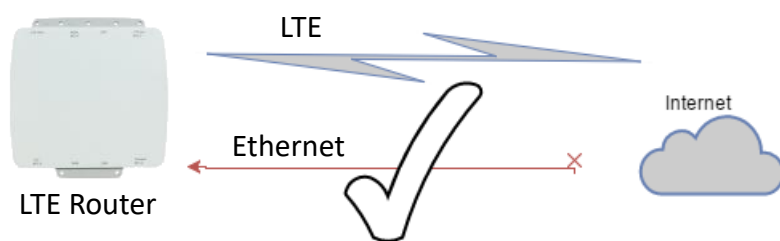
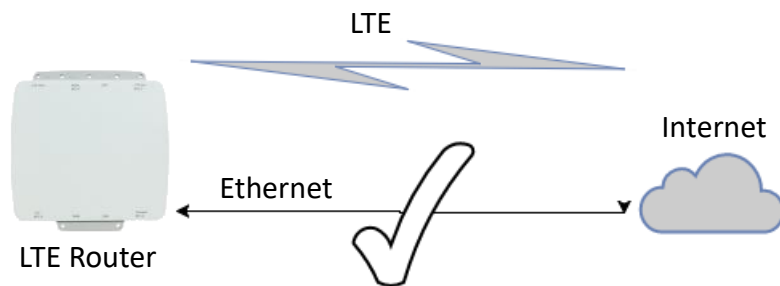
(2) WAN Priority > LTE Only:

In this mode, the router only routes network packages through LTE.



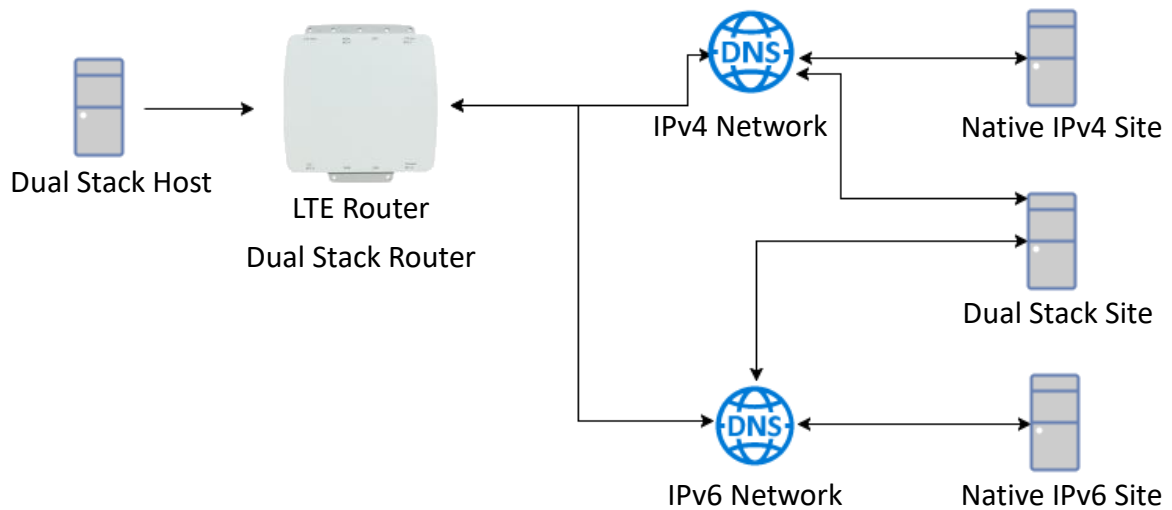
(3) WAN Priority > ETH Only:

In this mode, the router only routes network packages through Ethernet.



12.2 LAN > IPv4/IPv6 Dual Stack

The router supports IPv4/IPv6 dual stack by default, it means IPv4 packages route to IPv4 network and IPv6 route to IPv6 network.



Since IPv6 is global IP, there is no NAT between WAN site and LAN site. One device only needs one global IPv6. There is IPv6 firewall protection in the router by default. Only the IPv6 packages come from LAN site device and got reply back.

Status		
Attr.	Current SIM	Backup SIM
SIM Card	SIM1	SIM2
Modem Status	Ready	Not Inserted
Operator	Chunghwa Telecom	
Modem Access	FDD LTE	
IMSI	466924290307730	
Phone Number		
Band	LTE BAND 7	
Channel ID	3050	0
IPv4 Address	10.167.236.11	
IPv4 Mask	255.255.255.255	

Ethernet WAN	
Attr.	Value
IPv4 Address	192.168.11.176
IPv4 Mask	255.255.255.0

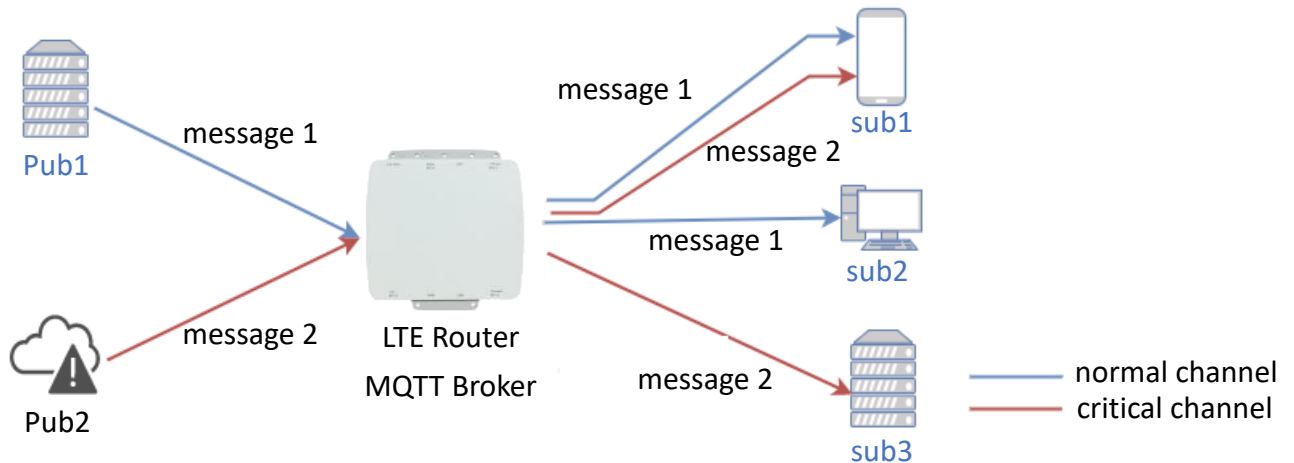
Ethernet LAN	
Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:b021:4a::100

The router automatically detects IPv6 environment and query IP. After the IP is obtained successfully, it will distribute to LAN site hosts.

12.3 MQTT Broker

The 4G/LTE Router provides the MQTT broker feature which allow the MQTT client sending the message within specific topic (channel).

By default, the 4G/LTE Router does not allow anonymous to read/write the MQTT topic (channel).



Thus, you need to create the account with username and password for MQTT client in the web UI.

The screenshot shows the MQTT web interface. At the top, there's a 'MQTT' header. Below it, the 'Mode' is set to 'Enable' (radio button selected) and the 'Port' is '1883'. The main section is titled 'Manage Users'. It contains a table with columns for 'Username', 'Password', and 'Delete'. The table lists five users: Sub1, Sub2, Sub3, Pub1, and Pub2. Each user has a corresponding password field (masked with dots) and a red 'Delete' button with an 'x' icon. Below the table, there are input fields for 'Username' and 'Password', and an 'Add' button.

Username	Password	Delete
Sub1	<input type="button" value="x"/>
Sub2	<input type="button" value="x"/>
Sub3	<input type="button" value="x"/>
Pub1	<input type="button" value="x"/>
Pub2	<input type="button" value="x"/>

The **Manage Users** section will show all created users. Each user can use the **delete** button to delete it.

For the ACL control, you can specify what topic should be limited.

For example, we set the publisher **pub1** to write the critical topic.

Additionally, we also the subscribers **sub1** and **sub3** can read the critical topic.

Thus, when **pub1** is sending the message only the **sub1**, the **sub3** can receive it.

ACLs

User	Topic	Read	Write	Delete
Sub1	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Sub3	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Pub2	Critical	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

User:

Topic:

Read

Write

12.4 OpenVPN Configuration

Generic setup

For OpenVPN configuration, use the certificate to authenticate the VPN connection.

Thus, you need to generate the required files for OpenVPN server or import the required file to OpenVPN client.

12.4.1 OpenVPN Server Mode

OpenVPN server certificate generation

Server - Server Security

Root CA

Cert, Key

Server - User Security

User 1	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 2	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 3	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 4	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 5	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 6	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 7	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>
User 8	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="text" value="password for create"/>

For the OpenVPN server mode, the OpenVPN web UI provides the buttons to generate the required files. The files include **Root CA**, **Cert**, **Key** and **OpenVPN** client files. The file will be generated when you click the corresponded **Create** button.

Note: The **Cert**, **Key** generation will take around 10 minutes.

To generate the OpenVPN client files, you need to type the password to create it.

The password will be used in the OpenVPN client when the client use **PKCS#12** to authenticate the VPN connection. After the generation, the web UI shows the below picture.

Server - Server Security

Root CA	Create	i	↓		
Cert, Key	Create	i Cert	↓	i Key	↓

Server - User Security

User 1	<input checked="" type="checkbox"/> Valid	Create	password for create	i Cert	↓	i Key	↓	i P12	↓
User 2	<input type="checkbox"/> Valid	Create	password for create						
User 3	<input type="checkbox"/> Valid	Create	password for create						
User 4	<input type="checkbox"/> Valid	Create	password for create						
User 5	<input type="checkbox"/> Valid	Create	password for create						
User 6	<input type="checkbox"/> Valid	Create	password for create						
User 7	<input type="checkbox"/> Valid	Create	password for create						
User 8	<input type="checkbox"/> Valid	Create	password for create						

And you can click the info button to show the detail for each files, or click the download button to download the file to PC.

12.4.2 OpenVPN Client Mode

OpenVPN client certificate import

For the OpenVPN client mode, the OpenVPN web UI provides the buttons to import the required files. The OpenVPN client can use the **Root CA**, **User Key** and **User Cert** files from OpenVPN server to authenticate the VPN tunnel. Or just only use the **PKCS#12 (P12)** file from OpenVPN server to authenticate it.

Note: The PKCS#12 files will contain the Root CA, User Key and User Cert.

When the files are imported, the web UI is as shown in the right-bottom picture.

Client - Security

Root CA	Import
Cert	Import
Key	Import
P12	Import

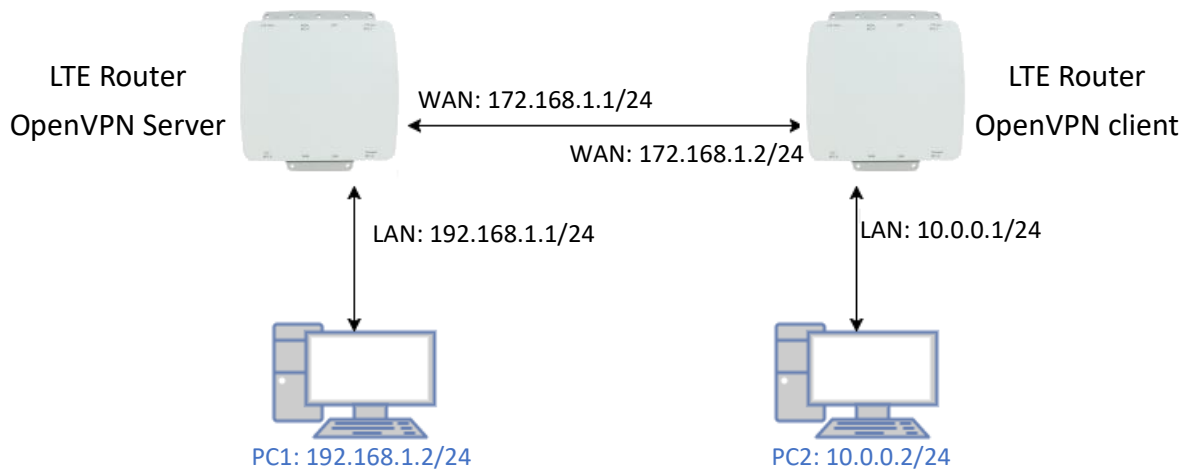
Client - Security

Root CA	Import	i	↓
Cert	Import	i	↓
Key	Import	i	↓
P12	Import	i	↓

Same as OpenVPN server part, you can use the info/download buttons to get the information of file or download the file to PC.

12.4.3 OpenVPN Net-to-Net

You can use the OpenVPN VPN tunnel to make the PC1 and PC2 communicate each other.



(1) OpenVPN server configuration

For the OpenVPN server side, the basic setting is as shown in below figure.

Edit Open VPN Connection #1

Mode Disable Enable

VPN Mode Server Client Custom

TLS Mode Disable Enable

TLS minimal version none 1.0 1.1 1.2

Cipher BF-CBC

Status Running

CN	IP	Connected since
user-00-00@openvpn	192.168.30.6	2017-06-21 10:38:13

Device TUN TAP

Protocol UDP TCP

Port 1701

VPN Compression Disable Enable

Authentication Certificate

Server

Client Mode Roadwarrior

VPN Network 192.168.30.0

VPN Netmask 255.255.255.0

Roadwarrior

Route Client Networks Off On

Connections - Net / Mask

#	Net / Mask
1	10.0.0.0 / 255.255.255.0

The **VPN Network** and **VPN Netmask** are required fields.

Note: The **VPN Network** should be network ID (e.g. **192.168.30.1** is invalid setting.)

When PC1 and PC2 communicate each other, the Route Client Networks should be enabled.

And add the LAN information of OpenVPN client side, in this case the **#1** route will be **10.0.0.0** and **255.255.255.0**

Note: The **#1** route means the routing information for **User 1**.

If all settings set up properly, the web UI will show the **Apply OK** and the OpenVPN server status should be **Running**. When OpenVPN Client mode is connected, the status will show the information which client is connected, IP address and connected time.

Status	Running	CN	IP	Connected since
		user-00-00@openvpn	192.168.30.6	2017-06-21 10:38:13

In the status, the **CN** field will indicate which client is connected and the **user-00-00@openvpn** value is from the **User 1** certificate information. You can check it by clicking the **information** button, the web UI will display the window as the below figure.

```
192.168.1.1/cgi-bin/openvpn.cgi?act=info&file=cert&type=user&conn_id=0&user_i...
192.168.1.1/cgi-bin/openvpn.cgi?act=info&file=cert&type=user&conn_id=0&user_id...

Certificate:
Data:
  Version: 1 (0x0)
  Serial Number: 1 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=CH, O=strongSwan, CN=OpenVPN
Validity
  Not Before: May 9 06:34:08 2017 GMT
  Not After : May 7 06:34:08 2027 GMT
  Subject: C=CH, O=strongSwan, CN=user-00-00@openvpn
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:ac:b1:ca:c7:74:18:70:ed:71:88:9e:c4:ba:d1:
      c4:09:52:b8:11:d7:17:00:e4:dd:e5:a7:f4:e1:f6:
      1c:10:b5:0c:d2:27:e7:f8:63:cb:e2:30:78:6c:ab:
      e3:eb:bd:08:a0:64:ed:1c:6d:97:8f:75:be:21:0d:
      47:1f:ca:66:6e:52:a8:c2:40:98:01:21:73:73:b5:
      62:c7:ab:a7:39:6b:94:7b:db:b4:a4:45:33:39:00:
      5b:92:f6:05:4c:18:e1:7d:1b:0b:35:ed:3b:da:0e:
      1c:f3:0e:db:04:e0:90:53:da:f5:87:91:d9:af:0f:
      3d:82:c3:12:ec:4a:e2:ed:77:d9:ca:89:2a:73:c9:
      e7:4f:a3:97:ff:97:f1:c4:f0:de:12:c0:ae:12:73:
      3f:63:30:dd:e8:87:97:59:34:e7:a7:1f:a0:53:c5:
      b1:f6:4d:10:2f:96:bd:f1:80:cc:62:5a:66:d8:30:
      29:c6:f3:fa:7a:69:4a:6a:67:0b:85:e7:8f:76:a4:
      fc:47:af:e5:1e:76:96:1c:f0:2b:64:d7:d0:02:50:
      63:43:ae:65:ad:88:73:b0:19:67:08:a4:60:6a:f1:
      03:93:62:f1:e3:0a:b3:70:82:dc:8b:85:a4:95:98:
      fb:f5:f8:81:2b:a5:55:8a:f7:1c:15:41:c2:f5:8b:
      ae:ed
    Exponent: 65537 (0x10001)
Signature Algorithm: sha256WithRSAEncryption
54:fd:09:0b:23:5b:d1:22:e3:17:1e:de:5c:48:1c:30:30:c7:
01:d8:6d:46:f4:91:4c:84:16:35:ea:79:91:67:dc:91:63:88:
6a:23:7b:fe:8c:e0:93:14:a1:1e:1d:32:c2:22:84:af:22:ff:
a9:9d:2f:aa:b2:0c:8b:86:c3:bc:46:8e:9d:5c:f8:55:39:91:
cc:03:17:40:e9:d5:bb:df:e9:34:aa:89:71:f7:ea:1c:78:78:
99:38:ba:7b:ec:d7:de:1a:d0:a0:07:58:cc:8a:4a:cc:2e:54:
b3:d9:46:03:8e:58:cb:ef:de:95:61:01:33:9f:40:4c:cb:1b:
3e:3e:70:4a:07:62:8c:d4:f0:53:86:42:c7:13:30:a8:3a:76:
d3:bf:9d:33:7b:50:c3:98:fd:f0:ed:2a:c3:00:b8:dc:e0:80:
a9:4b:0c:e1:ad:fc:32:76:03:b8:2f:9f:2a:d1:bb:1b:e7:cb:
62:d2:63:be:7c:21:ac:b5:91:14:55:96:fc:67:94:cc:1f:7b:
82:12:e6:84:da:fe:12:3e:73:bf:62:bb:1a:14:57:45:ce:28:
95:e1:1f:d9:86:cb:36:c6:4d:b8:04:af:f6:0e:f4:f4:31:ba:
6d:ef:cc:75:bc:0e:db:19:c7:c2:2c:b3:62:60:c2:88:d9:a3:
cf:d4:8b:25
-----BEGIN CERTIFICATE-----
MIIC5zCCA8CAQEwDQYJKoZIhvcNAQELBQAwNDELMAkGA1UEBhMCQ0gxExARBgNV
BAoMCmN0cm9uZ1N3YW4xEDAOBgNVBAMMB09wZjW5WUE4wHhcNMTCwNTA5MDYzNDA4
WhcNMicwNTA3MDYzNDA4WjA/MOSwCOYDVOOGEwJDSDETMBEGA1UECmKwC3Rvb25n
```

The CN information of user certificate is as shown in the subject field.

(2) OpenVPN client configuration

For the OpenVPN client side, the basic setting is as below figure.

The screenshot shows the 'Edit OpenVPN Connection #1' configuration page. It is divided into two main sections: the top section for general connection settings and the bottom section for client-specific settings.

General Connection Settings:

- Mode: Disable Enable
- VPN Mode: Server Client Custom
- TLS Mode: Disable Enable
- TLS minimal version: none 1.0 1.1 1.2
- Cipher: BF-CBC
- Status: Connected
- Device: TUN TAP
- Protocol: UDP TCP
- Port: 1701
- VPN Compression: Disable Enable
- Authentication: pkcs #12 Certificate

IP	Connected since
192.168.30.6	2017-06-21 10:38:15

Client Settings:

- Client Mode: Roadwarrior
- Server Address: 172.168.1.1
- PKCS12 Password: proscend
- Route Client Networks: Off On

The **Server Address** is required field, which indicate the OpenVPN server address which OpenVPN client try to connect. And the **PKCS12 Password** only works when selected the **pkcs #12 Certificate** authentication option.

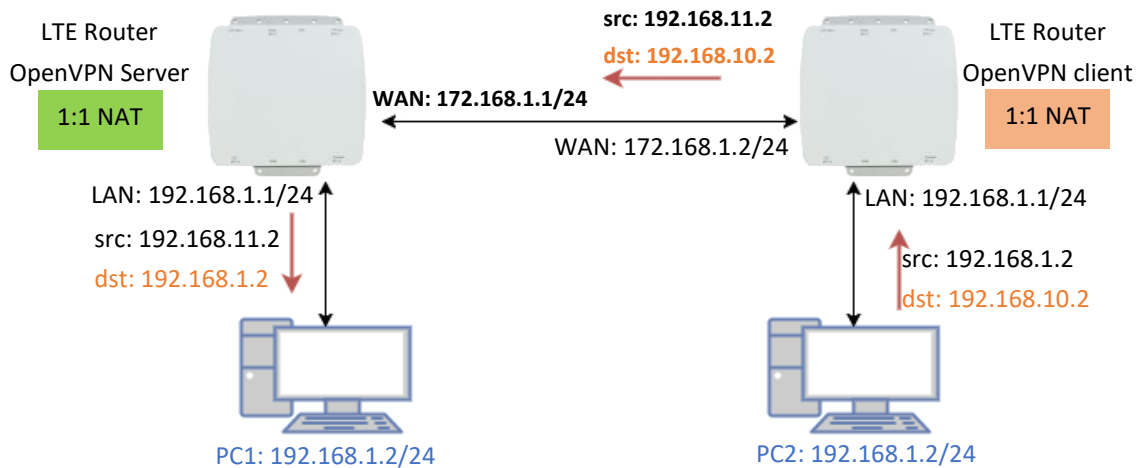
This option require the P12 file which generated from Generic Setup OpenVPN server part.

The password also be set on the Generic Setup OpenVPN server part.

If you use the Certificate authentication option, the OpenVPN client will require the **Root CA**, **User cert** and **User key** files.

Same as the OpenVPN server configuration part, OpenVPN client web UI also provides the status information. When all settings set up properly, the status will change from **Idle** to **Running**. When OpenVPN tunnel is created, the status shows **Connected** and the information for IP address and the time.

12.4.4 OpenVPN 1:1 NAT



For the net-to-net part, the OpenVPN server LAN network and the OpenVPN client LAN network are different. But some time, the LAN network will be same for both sides.

When this situation occurred, the routing rules will be ambiguous that will result in the PC1 and the PC2 can't communicate each other. Thus, the router OpenVPN provides the 1:1 NAT feature. The feature will convert the conflict subnet to different subnet. In this case, you can use 1:1 NAT feature to convert the LAN network of OpenVPN server and client.

For the server, we fill up the Network be **192.168.10.0** and Netmask **255.255.255.0**. The setting will make the router convert the server LAN network from **192.168.1.0/24** to **192.168.10.0/24** when the VPN traffic is coming.

Roadwarrior

Route Client Networks Off On

Connections - Net / Mask

#1	192.168.11.0	/	255.255.255.0
#2	0.0.0.0	/	0.0.0.0
#3	0.0.0.0	/	0.0.0.0
#4	0.0.0.0	/	0.0.0.0
#5	0.0.0.0	/	0.0.0.0
#6	0.0.0.0	/	0.0.0.0
#7	0.0.0.0	/	0.0.0.0
#8	0.0.0.0	/	0.0.0.0

NAT

1:1 NAT Off On

Network

Netmask

Per the OpenVPN client, same as server but we fill up the Network as **192.168.11.0**. This makes the router convert the client LAN network from **192.168.1.0/24** to **192.168.11.0/24** when the VPN traffic is coming.

Client

Client Mode Roadwarrior

Server Address

PKCS12 Password

Route Client Networks Off On

NAT

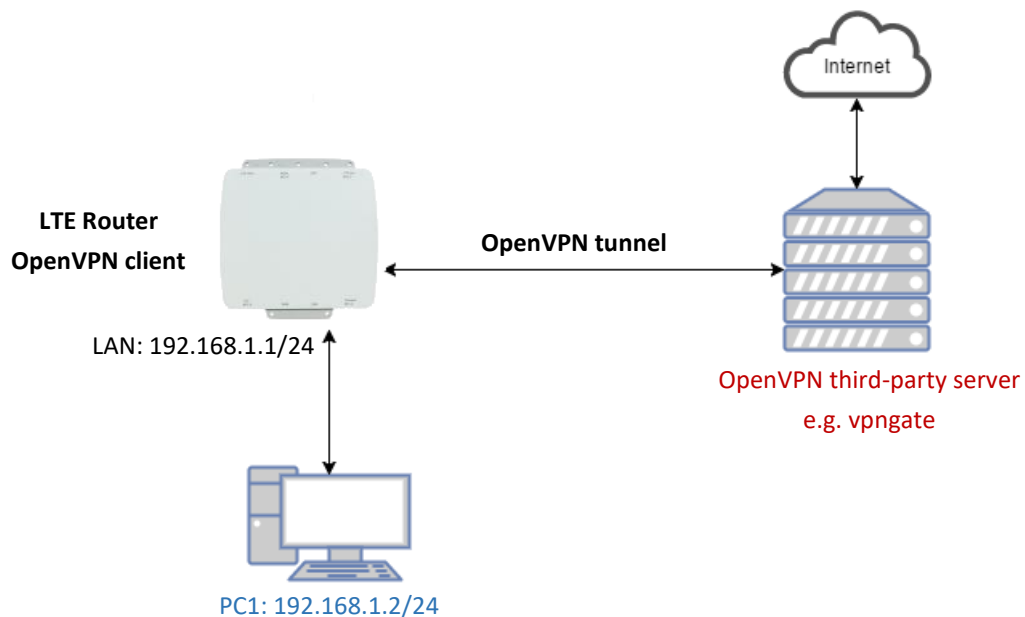
1:1 NAT Off On

Network

Netmask

The PC2 ping result:

12.4.5 OpenVPN with third-party server



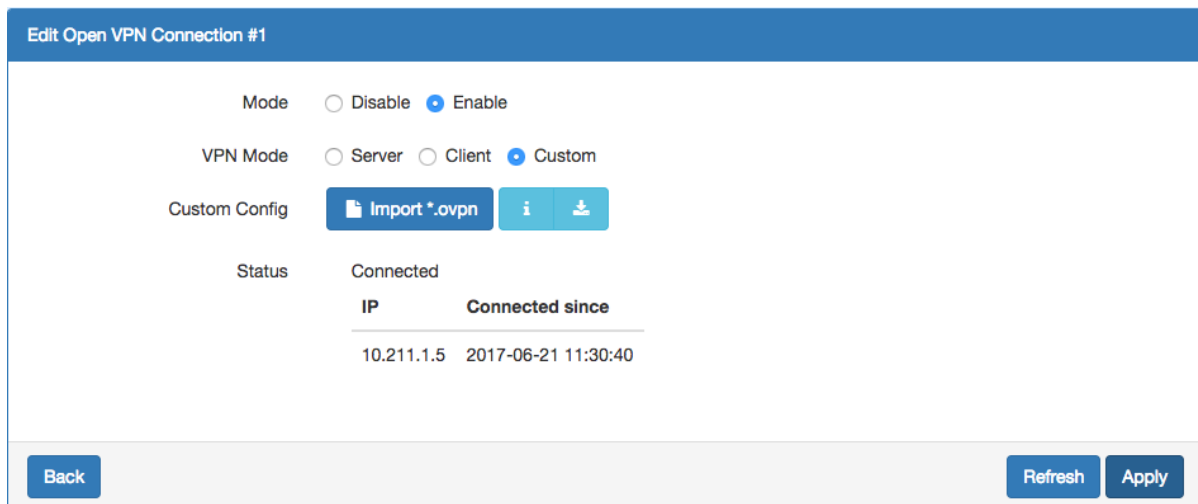
A VPN enables you to send and receive data across shared networks.

For some users, they will use the VPN to access the limited network service from the different country. But normally, the third-party OpenVPN server will provide the **.ovpn** configuration files for the OpenVPN client. The **.ovpn** is hard to convert to the 4G/LTE Router OpenVPN client configuration. So, we provide the **Custom** mode to make the user can easy use the **.ovpn** to set up the 4G/LTE Router OpenVPN client. The **Custom** mode provide the import button to allow user import the third-party OpenVPN server **.ovpn** configurations file.

For example, use the Japan OpenVPN server which provided by <http://www.vpngate.net/en/> .

Firstly, download the **.ovpn** configuration files from [vpngate.net](http://www.vpngate.net).

Additionally, use the OpenVPN custom import button to import it. The result is as the below figure. If the **.ovpn** configuration file is correct, the web UI will show **Apply OK**.

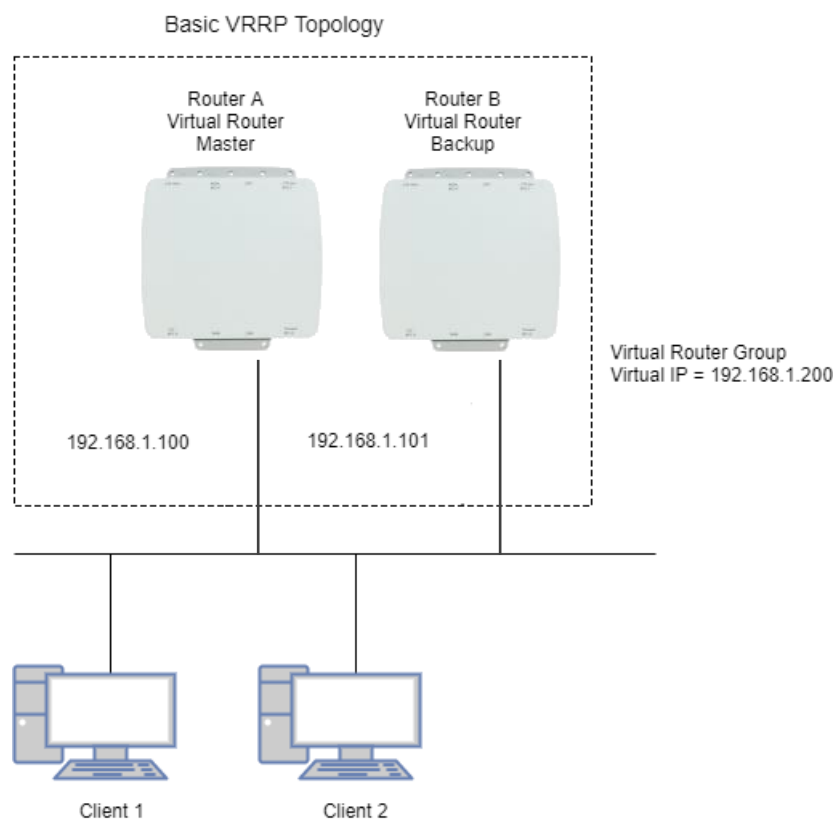


If the third-party OpenVPN server is reachable, the VPN tunnel will be established.

When the OpenVPN VPN tunnel is established, the status shows **Connected** and the information for IP address and the time. In this moment, the PC1 can visit the <http://www.vpngate.net> and the web UI should indicate the PC1 in the Japan at now as the below figure.

12.5 VRRP Topology

Basic VRRP Topology



Base on this topology and VRRP Parameter settings, Router A and Router B will offer a virtual router service with virtual IP = 192.168.1.200 for the client.

12.6 TR069 Server (GenieACS Installation)

Server OS: Ubuntu 14.04 on Virtualbox

Installation:

1) Login ubuntu

2) Change to root by 'su -' and enter your root password.

3) Install required package as below command:

```
>apt install gcc openssl-devel zlib-devel readline-devel sqlite-devel
```

4) Make a directory for application installation

```
>mkdir /opt
```

5) Install yaml

```
cd /opt
```

```
wget http://pyyaml.org/download/libyaml/yaml-0.1.7.tar.gz
```

```
tar xvzf yaml-0.1.7.tar.gz
```

```
cd yaml-0.1.7
```

```
./configure
```

```
make && make install
```

6) Install ruby

```
cd /opt
```

```
wget http://cache.ruby-lang.org/pub/ruby/2.4/ruby-2.4.1.tar.gz
```

```
tar xvzf ruby-2.4.1.tar.gz
```

```
cd ruby-2.4.1
```

```
./configure
```

```
make && make install
```

```
ruby -v
```

```
ruby 2.4.1p111 (2017-03-22 revision 58053) [i686-linux]
```

```
cd /opt
```

```
gem install rails --no-ri --no-rdoc
```

```
gem install bundle --no-ri --no-rdoc
```

7) Install node.js

```
cd /opt
```

```
wget http://nodejs.org/dist/v8.2.1/node-v8.2.1.tar.gz
```

```
tar zxvf node-v8.2.1.tar.gz
```

```
cd node-v8.2.1
```

```
./configure
```

```
make && make install
```

```
node -v
```

```
v8.2.1
```

8) Install redis

```
cd /opt
```

```
wget http://download.redis.io/releases/redis-4.0.1.tar.gz
tar zxvf redis-4.0.1.tar.gz
cd redis-4.0.1
make
make test
All tests passed without errors!
make install
#Start redis server
redis-server
```

9) Install mongodb

```
cd /opt
wget https://fastdl.mongodb.org/linux/mongodb-linux-i686-3.3.3.tgz
tar zxvf mongodb-linux-i686-3.3.3.tgz
cd mongodb-linux-i686-3.3.3
mkdir -p /data/db
```

10) Install genieACS

```
cd /opt
git clone https://github.com/zaidka/genieacs.git
cd genieacs
npm install
npm run configure
npm run compile
```

Modify FS_HOSTNAME field in genieacs/config/config.json for device retrieve firmware file

Original configuration:

```
"FS_HOSTNAME" : "acs.example.com"
```

New configuration example.:

```
"FS_HOSTNAME" : "192.168.0.199"
```

Note: It is the place where the device firmware file stored. Generally, it is the IP address on where your GenieACS server installed.

Modify connect request username/password in genieacs/config/auth.js to stimulate connection

Original configuration:

```
function connectionRequest(deviceId, url, username, password, callback) {
    return callback(username || deviceId, password || "");
}
```

New configuration example:

```
function connectionRequest(deviceId, url, username, password, callback) {
```

```
    return callback('tr069','tr069');
}
```

Note: The hard code username/password MUST same with device's connection request username/password, otherwise the ACS stimulate connection will fail.

11) Install genieACS-Gui

```
git clone https://github.com/zaidka/genieacs-gui
cd genieacs-gui
bundle
```

```
gem install json
bundle update
```

```
rm -f db/*.sqlite3
rake db:create
RAILS_ENV=development rake db:migrate
```

```
cd /opt
cd genieacs-gui/config
cp index_parameters-sample.yml index_parameters.yml
cp parameter_renderers-sample.yml parameter_renderers.yml
cp parameters_edit-sample.yml parameters_edit.yml
cp roles-sample.yml roles.yml
cp summary_parameters-sample.yml summary_parameters.yml
cp users-sample.yml users.yml
cp graphs-sample.json.erb graphs.json.erb
```

GenieACS startup script:

```
#!/bin/sh
```

```
GENIE_PATH=/opt/genieacs/bin
GENIE_GUI_PATH=/opt/genieacs-gui
```

```
echo "start mongod."
pidof mongod
if [ $? != 0 ]; then
/opt/mongodb-linux-i686-3.3.3/bin/mongod --dbpath /data/db --journal --storageEngine=mmapv1 --fork
--syslog
fi
```

```
echo "start North Bound/RESTful Interface service."
$GENIE_PATH/genieacs-nbi &
```

```
echo "start ACS/CWMP service."
$GENIE_PATH/genieacs-cwmp &
```

```
echo "start HTTP/File streaming service."
$GENIE_PATH/genieacs-fs &
```

```
echo "start GenieACS/WebUI."
cd $GENIE_GUI_PATH
rails server -b 0.0.0.0
```

GenieACS stop:

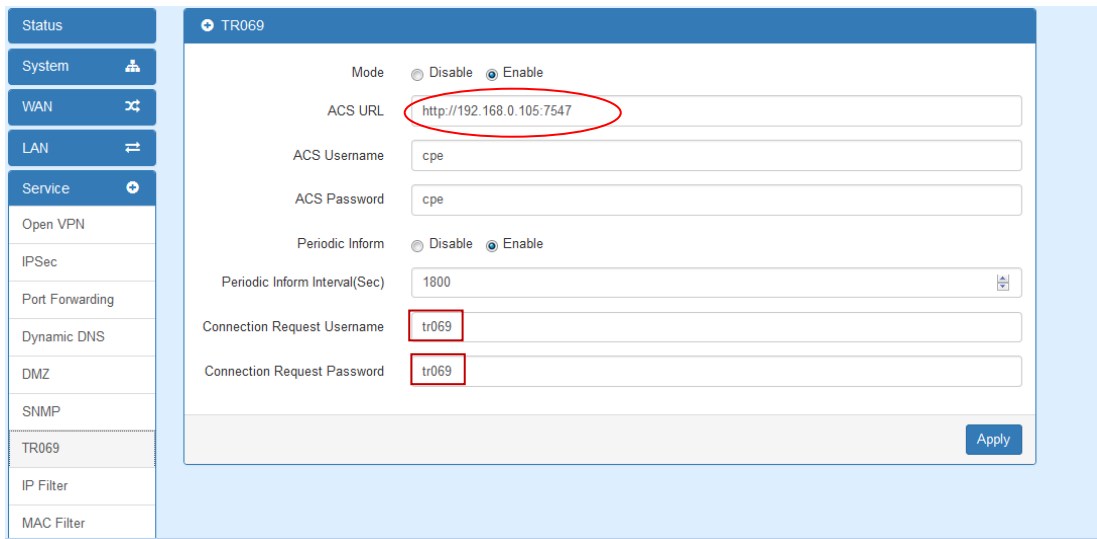
Ctrl-C

Usage:

1) Device Configuration

Fill in the ACS URL field as <http://GenieACS server IP:7547>

Fill in the Connection Request Username and Connection Request Password fields to same with the configuration in `genieacs/config/auth.js`.

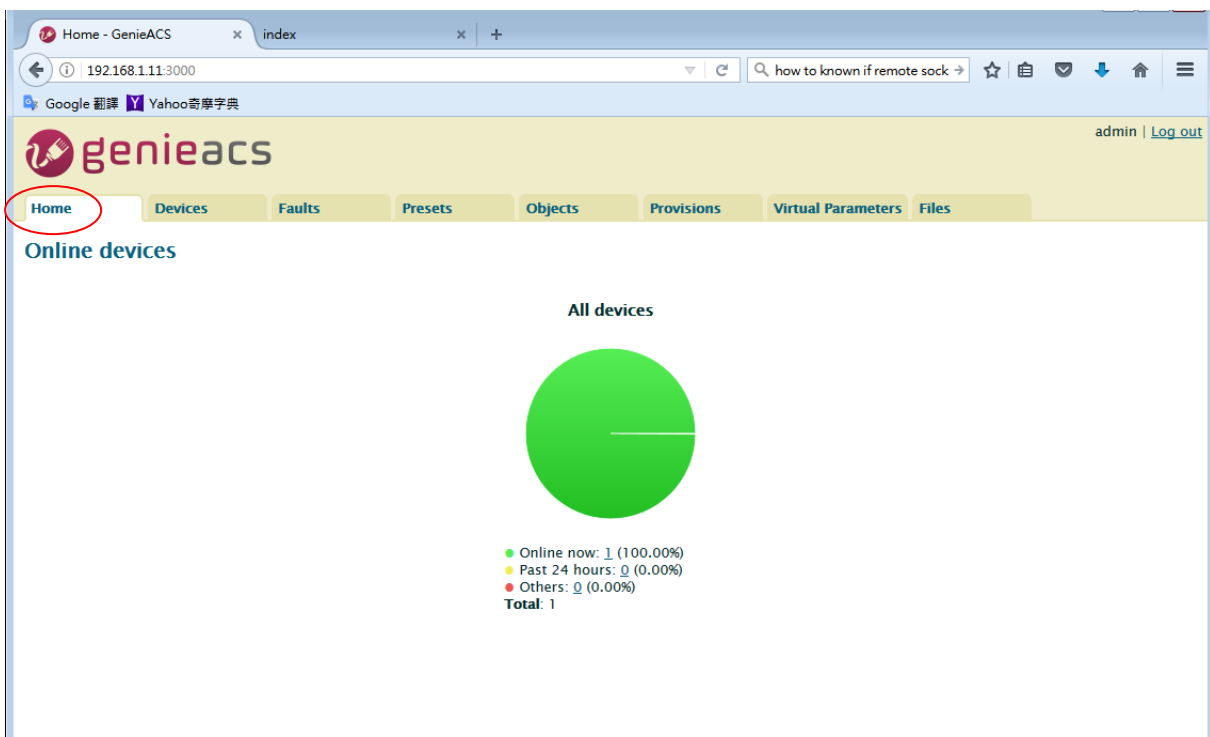


The screenshot shows the configuration page for TR069. The Mode is set to Enable. The ACS URL is `http://192.168.0.105:7547`. The ACS Username and ACS Password are both `cpe`. The Periodic Inform is set to Enable with an interval of 1800 seconds. The Connection Request Username and Connection Request Password are both `tr069`. An Apply button is visible at the bottom right.

2) GenieACS Operation

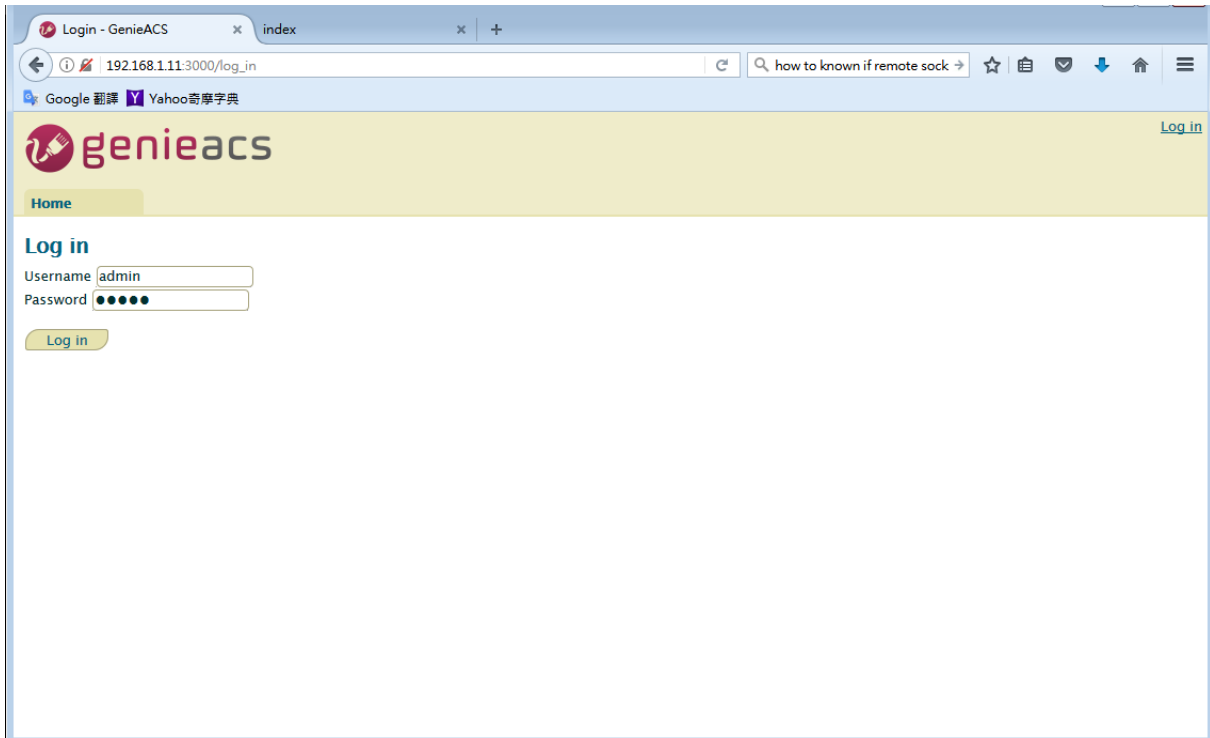
Input `http://GenieACS server IP:3000` on browser url bar and Enter.

Press Home tab to refresh Online devices status.



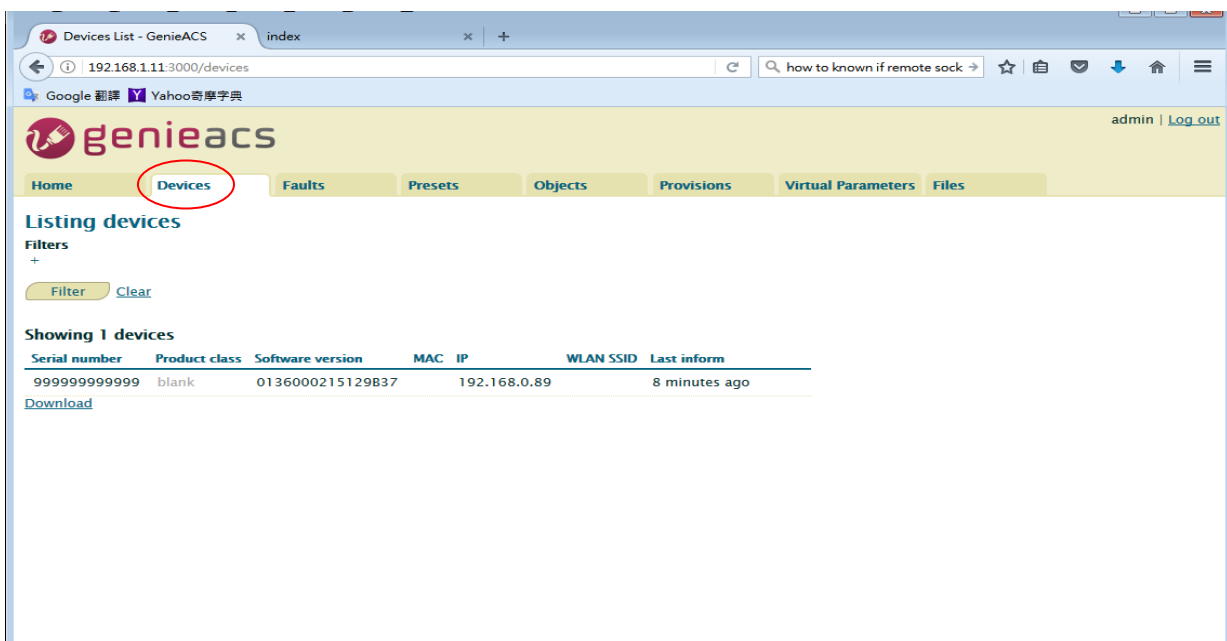
2.1) Login

Username and Password are admin/admin.



3) Device information

Press Devices tab



Move mouse to line end of your device, the [Show](#) link show up.

Showing 1 devices

Serial number	Product class	Software version	MAC	IP	WLAN SSID	Last inform
999999999999	blank	0136000215129B37		192.168.0.89		8 minutes ago

Download

Press [Show](#) link, the device information show up.

admin | [Log out](#)

[Home](#) [Devices](#) [Faults](#) [Presets](#) [Objects](#) [Provisions](#) [Virtual Parameters](#) [Files](#)

Device: 00304F-999999999999
Tags: +
Last inform: 12 minutes ago — Refresh, Ping

Serial number: 999999999999
Product class: blank
OUI: 00304F
Manufacturer: Generic
Hardware version: 0136000200000000
Software version: 0136000215129B37
IP: 192.168.0.89 — [Edit](#)

Task queue
Task Time Fault code Fault message Fault detail Retries
Empty

Device parameters
Type to search...
InternetGatewayDevice
InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[(Baseline:1,Eth...
InternetGatewayDevice.DeviceInfo
InternetGatewayDevice.DeviceInfo.SpecVersion 1.0
InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000
InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129B37
InternetGatewayDevice.DeviceInfo.ProvisioningCode blank
InternetGatewayDevice.DeviceInfo.AdditionalSoftwareVersion V.51
InternetGatewayDevice.DeviceInfo.ManufacturerOUI 00304F
InternetGatewayDevice.DeviceInfo.ModelName <UNKNOWN>
InternetGatewayDevice.DeviceInfo.Description Generic
InternetGatewayDevice.DeviceInfo.ProductClass blank

[Reboot](#)
[Factory reset](#)
[Push file](#)
[Add Firmware](#)
[Delete](#)

4) Access parameters

Scroll up/down on Device parameters list, the [Refresh](#) and [Edit](#) link show up at line end of parameter.

For Readable parameter

Device parameters
Type to search...
InternetGatewayDevice
InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[(Baseline:1,Eth...
InternetGatewayDevice.DeviceInfo
InternetGatewayDevice.DeviceInfo.SpecVersion 1.0
InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000 [Refresh](#)
InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129B37
InternetGatewayDevice.DeviceInfo.ProvisioningCode blank

For Readable

and Writable parameter

InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dest 0.0.0.0
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_begin 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_end 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.16
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.mode **off** [Edit](#) [Refresh](#)
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.description blank
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.protocol tcp
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_begin 0

4.1) Get parameter value

Press on the [Refresh](#) link, the Pending tasks window will popup on right top to ask you to allow or Cancel this action.

genieacs admin | Log out

Home Devices **Faults** Presets Objects Provisions Vi

Device: 00304F-999999999999

Tags: +

Last inform: 12 minutes ago — Refresh, Ping

Serial number: 999999999999
 Product class: blank
 OUI: 00304F
 Manufacturer: Generic
 Hardware version: 0136000200000000
 Software version: 0136000215129B37
 IP: 192.168.0.89 — Edit

Task queue

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

Type to search...

- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.protocol tcp
- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.sport_begin 0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.sport_end 0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dest 0.0.0.0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_begin 0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_end 0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16.mode off
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16.description blank
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16.protocol tcp
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_begin 0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_end 0

Reboot
 Factory reset
 Push file >
 Add Firmware
 Delete

Press Commit to get this parameter value.

Note: If the GenieACS can reach the device, the parameter value will be updated immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.

Note: To update the whole tree, refresh the root parameter (InternetGatewayDevice.).

Note: To update partial tree, refresh the parent node of the partial tree.

4.2) Set parameter value

Press on the **Edit** link, Editing window will pop up to ask you to change the value of this parameter.

genieacs admin | Log out

Home Devices **Faults** Presets Objects Provisions **Virtual Parameters** Files

Device is offline

Device: 00304F-999999999999

Tags: +

Last inform: less than 5 seconds ago — Refresh, Ping

Serial number: 999999999999
 Product class: blank
 OUI: 00304F
 Manufacturer: Generic
 Hardware version: 0136000200000000
 Software version: 0136000215129B37
 IP: 192.168.0.89 — Edit

Task queue

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

Type to search...

- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.protocol tcp
- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.sport_begin 0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.sport_end 0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dest 0.0.0.0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_begin 0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_end 0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16.mode off
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16.description blank
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16.protocol tcp
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_begin 0
- InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_end 0

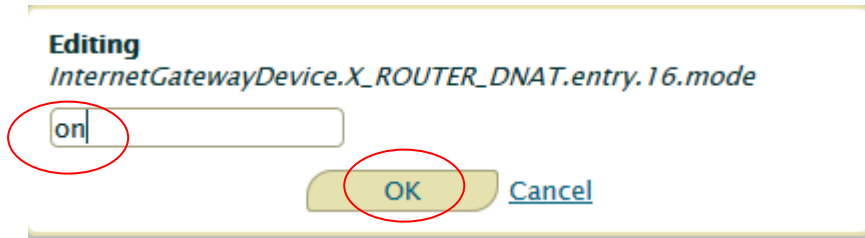
Reboot
 Factory reset
 Push file >
 Add Firmware
 Delete

Editing
 InternetGatewayDevice.X_ROUTER_DNAT.entry.16.mode

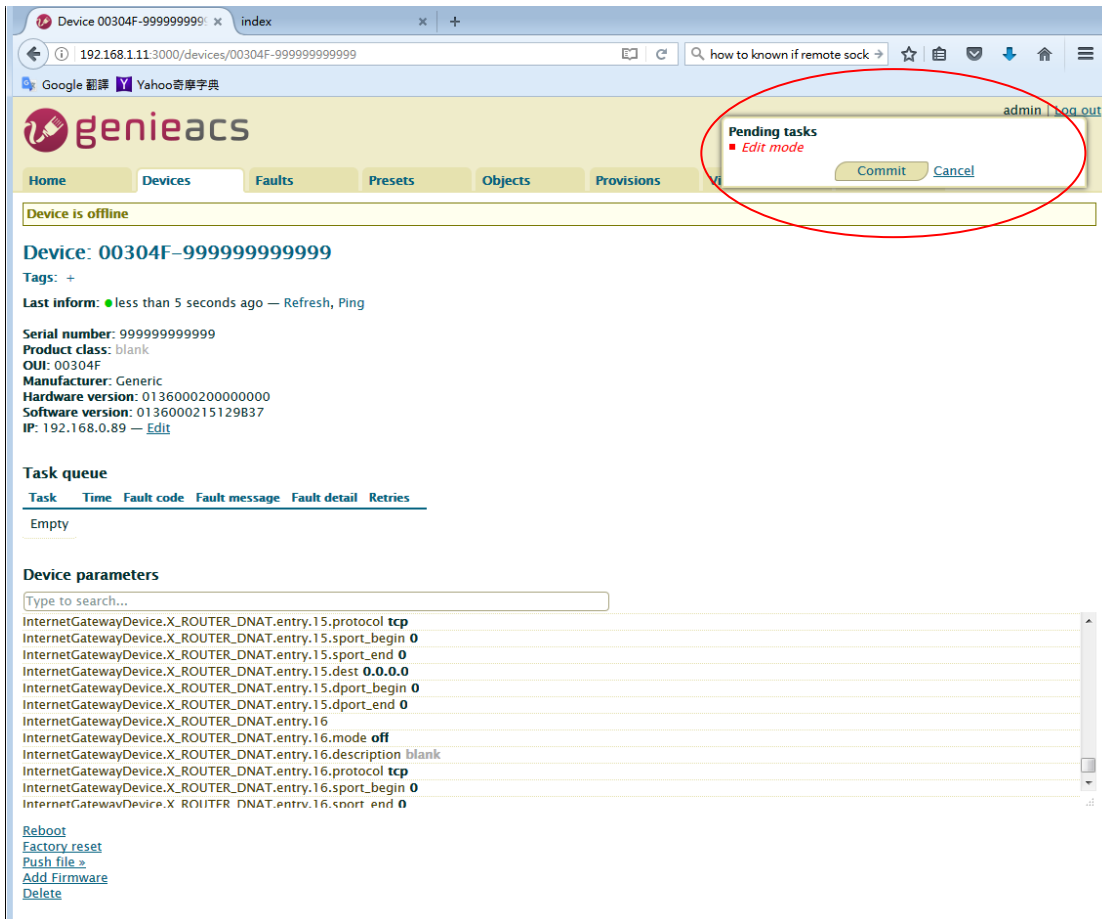
off

OK Cancel

Input new value and press OK.



The Pending tasks window will pop up to ask you to allow or Cancel this action.



Press Commit to set this parameter value.

Note: If the GenieACS can reach the device, the parameter value will be set immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.

5) Reboot device

Press on [Reboot](#) link.

The Pending tasks window will popup to ask you to allow or Cancel this action.

Press Commit to reboot device.

Note: If the GenieACS can reach the device, the device will reboot immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.

6) Reset to default

Similar to Reboot device except pressing on [Factory reset](#) link.

7) Firmware Upgrade

7.1) Upload Firmware

Press [Add Firmware](#) link

admin | [Log out](#)

Home Devices **Faults** Presets Objects Provisions Virtual Parameters Files

Device: 00304F-Mobile%20Router-9999999999

Tags: +

Last inform: about 2 hours ago — Refresh, Ping

Serial number: 999999999999
 Product class: Mobile Router
 OUI: 00304F
 Manufacturer: Generic
 Hardware version: 0136000200000000
 Software version: 0136000215129839
 IP: 192.168.0.89 — [Edit](#)

Task queue

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

Type to search...

InternetGatewayDevice
 InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[(Baseline:1,Eth...
 InternetGatewayDevice.DeviceInfo
 InternetGatewayDevice.DeviceInfo.SpecVersion 1.0
 InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000
 InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129839
 InternetGatewayDevice.DeviceInfo.ProvisioningCode blank
 InternetGatewayDevice.DeviceInfo.Manufacturer Generic
 InternetGatewayDevice.DeviceInfo.UpTime 3920 (1:5:20)
 InternetGatewayDevice.DeviceInfo.AdditionalSoftwareVersion V1.51
 InternetGatewayDevice.DeviceInfo.ModemFirmwareVersion EC25EFAR02A06M4G
 InternetGatewayDevice.DeviceInfo.SerialNumber 999999999999

[Reboot](#)
[Factory reset](#)
[Push file >>](#)
[Add Firmware](#)
[Delete](#)

The link will redirect to Files tab

admin | [Log out](#)

Home Devices Faults Presets Objects Provisions Virtual Parameters **Files**

New file

File type: 1 Firmware Upgrade Image

OUI: 00304F

Product class: Mobile Router

Version: 0136000215129839

File:

Press File: browse button, select the firmware, and then press Upload button.

The firmware will be added to Listing files as below.

admin | [Log out](#)

Home Devices Faults Presets Objects Provisions Virtual Parameters **Files**

Listing files

Showing 1 files

Name	Type	OUI	Product class	Version
m300.img	1 Firmware Upgrade Image	00304F	Mobile Router	0136000215129839

[New File](#)

7.2) Upgrade

Move mouse to the [Push file>>](#) link, the upgrade firmware name will pop up as below picture.

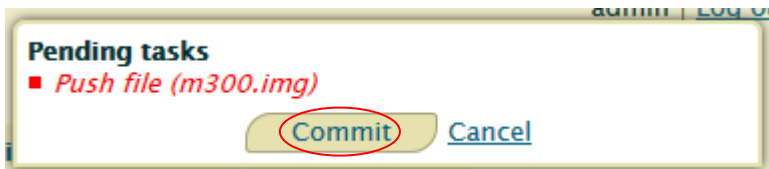
Device parameters

Type to search...

InternetGatewayDevice
InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[(Baseline:1,Eth...
InternetGatewayDevice.DeviceInfo
InternetGatewayDevice.DeviceInfo.SpecVersion 1.0
InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000
InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129B39
InternetGatewayDevice.DeviceInfo.ProvisioningCode blank
InternetGatewayDevice.DeviceInfo.Manufacturer Generic
InternetGatewayDevice.DeviceInfo.UpTime 1020 (0:17:0)
InternetGatewayDevice.DeviceInfo.AdditionalSoftwareVersion V1.51
InternetGatewayDevice.DeviceInfo.ModemFirmwareVersion EC25EFAR02A06M4G
InternetGatewayDevice.DeviceInfo.SerialNumber 999999999999

[Reboot](#)
[Factory reset](#)
[Push file](#) **m300.img (1 Firmware Upgrade Image)**
[Add Firmware](#)
[Delete](#)

Move mouse to the upgrade firmware name and press it. The Pending tasks window will pop up to ask you to allow or Cancel this action.



Press Commit, then firmware upgrade started.

Note: If the GenieACS can reach the device, the firmware upgrade will be started immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.